LOAN DOCUMENT

PHOTOGRAPH THIS SHEET

DTIC ACCESSION NUMBER

LEVEL

INVENTORY 0

PNL-6890
DOCUMENT IDENTIFICATION
MAY 1989

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DISTRIBUTION STATEMENT

HANDLE WITH CARE

ACCESSION FOR
NTIS GRA&I
DTIC TRAC
UNANNOUNCED
JUSTIFICATION

BY
DISTRIBUTION/
AVAILABILITY CODES

DISTRIBUTION	AVAILABILITY AND/OR SPECIAL	
A-1		

DISTRIBUTION STAMP

DATE ACCESSIONED

DATE RETURNED

20000203 051

DATE RECEIVED IN DTIC

REGISTERED OR CERTIFIED NUMBER

PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-FDAC

DTIC FORM 70A JUN 90

DOCUMENT PROCESSING SHEET

PREVIOUS EDITIONS MAY BE USED UNTIL STOCK IS EXHAUSTED.

LOAN DOCUMENT

PNL-6890
UC-706

FINAL REPORT

System Safety Management Lessons Learned

May 1989

Prepared for the
U.S. Army Safety Center
Ft. Rucker, Alabama
under a Related Services Agreement
with the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Operated for the U.S. Department of Energy
by Battelle Memorial Institute

Battelle

PNL-6890

DISCLAIMER

PACIFIC NORTHWEST LABORATORY
operated by
BATTELLE MEMORIAL INSTITUTE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RLO 1830

Printed in the United States of America
Available from
National Technical Information Service
United States Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161

NTIS Price Codes
Microfiche A01

Printed Copy

Pages	Price Codes
001-025	A02
026-050	A03
051-075	A04
076-100	A05
101-125	A06
126-150	A07
151-175	A08
176-200	A09
201-225	A10
226-250	A11
251-275	A12
276-300	A13

FOR FURTHUR INFORMATION CONCERNING DISTRIBUTION CALL (703) 767-8040

PLEASE CHECK THE APPROPRIATE BLOCK BELOW:

AQ #_____

☐ _____ copies are being forwarded. Indicate whether Statement A. B. C. D. E, F. or X applies.

☑ DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

☐ DISTRIBUTION STATEMENT B:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES ONLY; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT C:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT D:
DISTRIBUTION AUTHORIZED TO DoD AND U.S. DoD CONTRACTORS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT E:
DISTRIBUTION AUTHORIZED TO DoD COMPONENTS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT F:
FURTHER DISSEMINATION ONLY AS DIRECTED BY (Indicate Controlling DoD Office and Date) or HIGHER DoD AUTHORITY.

☐ DISTRIBUTION STATEMENT X:
DISTRIBUTION AUTHORIZED TO U.S GOVERNMENT AGENCIES AND PRIVATE INDIVIDUALS OR ENTERPRISES ELIGIBLE TO OBTAIN EXPORT-CONTROLLED TECHNICAL DATA IN ACCORDANCE WITH DoD DIRECTIVE 5230.25. WITHHOLDING OF UNCLASSIFIED TECHNICAL DAT \FROM PUBLIC DISCLOSURE. 6 Nov 1984 (indicate date of determination). CONTROLLING DoD OFFICE IS (Indicate Controlling DoD Office).

☐ This document was previously forwarded to DTIC on _____ (date) and the AD number is _____

☐ In accordance with provisions of DoD instructions. the document requested is not supplied because:

☐ It will be published at a later date. (Enter approximate date. if known).

☐ Other. (Give Reason)

DoD Directive 5230.24, "Distribution Statements on Technical Documents," 18 Mar 87, contains seven distribution statements, as described briefly above. Technical Documents must be assigned distribution statements.

Cynthia Gleisberg
Print or Type Name

334-255-2924
Telephone Number

Cynthia Gleisberg
Authorized Signature/Date

PNL-6890
UC-706

System Safety Management Lessons Learned

J.A. Piatt
Principal Investigator

Technical Contributors:
J. M. Grass
M. S. Harris
T.C. Krenelka
J. C. Lavender
D. A. Seaver

May 1989

Prepared for the
U.S. Army Safety Center
Ft. Rucker, Alabama
under a Related Services Agreement
with theU.S. Department of Energy
Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Richland, Washington 99352

Executive Summary

The Assistant Secretary of the Army for Research, Development and Acquisition directed the Army Safety Center to provide an audit of the causes of accidents and safety of use restrictions on recently fielded systems by tracking residual hazards back through the acquisition process. The objective was to develop "lessons learned" that could be applied to the acquisition process to minimize mishaps in fielded systems. System safety management lessons learned are defined as Army practices or policies, derived from past successes and failures, that are expected to be effective in eliminating or reducing specific systemic causes of residual hazards. They are broadly applicable and supportive of the Army structure and acquisition objectives.

Pacific Northwest Laboratory (PNL)[a] was given the task of conducting an independent, objective appraisal of the Army's system safety program in the context of the Army materiel acquisition process by focusing on four fielded systems which are products of that process.These systems included the Apache helicopter, the Bradley Fighting Vehicle(BFV), the Tube Launched, Optically Tracked, Wire Guided (TOW) Missile and the HIgh Mobility Multipurpose Wheeled Vehicle (HMMWV). The objective of this study was to develop system safety management lessons learned associated with the acquisition process.

The first step was to identify residual hazards associated with the selected systems. Since it was impossible to track all residual hazards through the acquisition process, certain well-known, high visibility hazards were selected for detailed tracking. These residual hazards illustrate a variety of systemic problems. Systemic or process causes were identified for each residual hazard and analyzed to determine why they exist. System safety management lessons learned were developed to address related systemic causal factors.

System Safety Management Lessons Learned

For the purposes of this study, residual hazards were defined as conditions associated with fielded systems that could result in injury, illness, death or damage to or loss of equipment or property. PNL has identified fourteen lessons learned. These lessons learned were derived from the systemic causes of specific hazards and the reasons that these causes exist. Recommendations resulting from the following system safety management lessons learned address the major systemic causes of residual hazards.

- The role of Army system safety professionals must strike a balance between oversight and increased direct involvement in system acquisition to make the best use of limited system safety resources.
- System safety training should be provided for all supporting acquisition players to provide a proper understanding of their system safety roles and objectives.
- Plans for implementing a system safety program within Project Management Offices (PMOs) should be based on projected life-cycle losses of the systems being acquired. System safety efforts must be initiated early in the acquisition process to produce minimum risk systems
- Requirements for system safety resources and the means of providing those resources should be established at the outset of the acquisition program. To provide the necessary resources for PMOs, contracts should be considered to supplement existing system safety support. Allocation of Army system safety resources should be based on commodity risks.
- Designers must be aware of historic and state-of-the-art system safety design guidance to improve the safety of new generations of Army materiel.
- Since human error is a contributing cause in a majority of Army mishaps, human performance limitations must receive greater consideration during the selection and evaluation of control measures for severe hazards. Human factors engineers should review user-dependent hazard control measures to ensure that they are reasonable and effective.
- The Army must promote greater customer participation in the system safety program to ensure realistic control of hazards in the use environment and enhanced mission performance.

(a) Pacific Northwest Laboratory is operated for the U.S. Department of Energy by Battelle Memorial Institute.

- Hazard probability must be expressed as a quantitative rate and interpreted in light of exposure in order to be useful in projecting losses for risk-management decisions. Provide a standard method of predicting human reliability to reduce errors in assessing hazard probabilities involving human performance.
- Control measures for severe hazards (catastrophic and critical) must be systematically verified during testing.
- Safety risks should be communicated to decision makers in terms of projected loss rates and programmatic and mission impacts that may be expected if a hazard is accepted.
- Risk management decisions must be made at a management level commensurate with risk and documented.
- All the players in the acquisition process must have access to relevant hazard information to do their jobs properly. Significant system safety documentation must be maintained for comparison of risk management expectations with the safety performance of the fielded systems and for development of lessons learned.
- There must be a systematic hazard closeout process to ensure that necessary steps for hazard resolution are not overlooked.
- The system safety performance of acquisition managers and contractors must be routinely evaluated. Investigate the feasibility of using performance award contracts to reward system safety excellence.

Specific changes to Army policy and guidance documents necessary to implement these lessons learned are provided in Appendix A of the report.

Conclusions

This study has confirmed that many contributing causes of residual hazards can be traced back to the acquisition process and the system safety program, which is part of that process. System safety management lessons learned can be derived from these systemic causes. Implementation of the recommendations from these system safety management lessons learned will support acquisition managers, because the lessons learned 1) contribute to operational effectiveness of Army systems by reducing the potential for mishaps, 2) reduce system costs by reducing safety-related retrofit and life-cycle mishap costs, and 3) reduce program delays and restrictions of fielded systems by ensuring better communication of system safety expectations to developers and earlier verification of the adequacy of hazard control measures.

Acronyms and Abbreviations

AAE	Army Acquisition Executive
AMC	U.S. Army Materiel Command
AMSAA	U.S. Army Materiel Systems Analysis Activity
ASARC	Army Systems Acquisition Review Council
ASMIS	Army Safety Management Information System
AVSCOM	U.S. Aviation Systems Command
BFV	Bradley Fighting Vehicle
DA	Department of the Army
DoD	Department of Defense
DRS	Deficiency Reporting System
EIR	Equipment Improvement Recommendation
HMMWV	High Mobility Multipurpose Wheeled Vehicle
LABCOM	U.S. Army Laboratory Command
MACOM	Major Army Command
MADP	Materiel Acquisition Decision Process
MANPRINT	Manpower and Personnel Integration
MICOM	U.S. Army Missile Command
MOS	Military Occupational Specialty
MRSA	U.S. Army Materiel Readiness Support Activity
MSC	Major Subordinate Command
PEO	Program Executive Officer
OTEA	U.S. Army Operational Test and Evaluation Agency
PM	Program/Project/ Product Manager
PMO	Program Management Office
PNL	Pacific Northwest Laboratory
QDR	Quality Deficiency Report
RFP	Request for Proposal
ROC	Required Operational Capability
SAR	Safety Assessment Report
SSWG	System Safety Working Group
TACOM	U.S. Army Tank-Automotive Command
TECOM	U.S. Army Test and Evaluation Command
TM	Technical Manual
TRADOC	U.S. Army Training and Doctrine Command
TOP	Test Operations Procedure
TOW	Tube Launched, Optically Tracked, Wire Guided (Missile)
USASC	U.S. Army Safety Center

Acknowledgments

The authors wish to acknowledge the support and cooperation of the many individuals at the project management offices, safety offices, field sites and the U.S. Army Safety Center who helped to provide the necessary information to enable us to meet the objectives of this study. We are also indebted to the capable assistance of the technical and executive subpanels of the Department of the Army System Safety Coordinating Panel in providing valuable comments on the draft report.

Table of Contents

1.0 Introduction

The U.S. Army has established a comprehensive safety program to minimize the loss of human and material resources. Data on the frequency and severity of mishaps involving newly developed and fielded systems indicate that such losses continue to be a significant contributor to overall Army mishap losses. It was hypothesized that the root causes of such mishaps are systemic in nature and involve fundamental processes of the materiel acquisition process and the system safety program.

The Assistant Secretary of the Army for Research, Development and Acquisition, ASA(RDA), Dr. Jay Sculley, directed an *"...audit of causes for accidents and safety of use restrictions on our recently fielded systems. This audit would track the actual causes back through the system safety reviews and analyses during the design phases to see how the potential for their eventual accident causes was assessed and what preventative action, if any, was taken. The desired result is 'lessons learned' for use in our new system."* (a)

The directive recognizes that the causes of accidents and the causes of restrictions in safety messages are the same. Safety-of-Use and Safety-of-Flight messages and restrictions are symtomatic of problems with the acquisition process and system safety program; they are not a problem in and of themselves. Eliminating the causes of residual hazards will in turn reduce the number of safety messages and restrictions. Pressure to unilaterally reduce the number of safety messages might well increase any Army mishap losses.

System safety management lessons learned are defined as Army practices or policies, derived from past successes and failures, that are expected to be effective in eliminating or reducing specific systemic causes of residual hazards. They are broadly applicable and supportive of the Army structure and acquisition objectives.

1.1 Objective

The ultimate goal of a comprehensive system safety program is to minimize mishaps and thus maximize operational effectiveness of Army materiel. The objective of the study was to develop system safety management "lessons learned" to support the Army's development of an optimum management strategy to meet this goal. The following activities were conducted in support of this objective:

a.) identification of residual hazards associated with four selected systems

b.) identification of problems and successes involving fundamental processes that permit or prevent systems from being fielded with residual hazards

c.) development of system safety management lessons learned based on the identified causes of past problems and successes

d.) preparation of a matrix of system safety management lessons learned and the status of their implementation in current Army policy and guidance documents

e.) development of specific recommendations for improving the system safety program and the materiel acquisition process to minimize residual hazards and subsequent mishaps after systems are fielded.

Completion of these activities sequentially moved from a system-specific to a process-specific orientation, as shown in Figure 1.

1.2 Scope

This study was authorized to examine any portion of the acquisition process and any Army policy that has an impact on the safety of fielded systems. Therefore, the lessons learned involve not only system safety personnel, but the entire acquisition community and their individual contributions to the safety of fielded systems. Figure 2 shows the four systems selected for this study.

Three systems were initially recommended by the U.S. Army Safety Center (USASC): the Bradley Fighting Vehicle, the Apache, and the TOW missile system. In response to a recommendation from the Executive Subpanel of the Department of the Army System Safety Coordinating Panel at its meeting January 6, 1988, the High Mobility Multipurpose Wheeled Vehicle was added to provide a representative non-major system for this study.

These systems have a high fielded density and represent several different commodities. They all had system safety

(a) Letter, System Safety Programs, ASA(RDA), 11 August 1987.

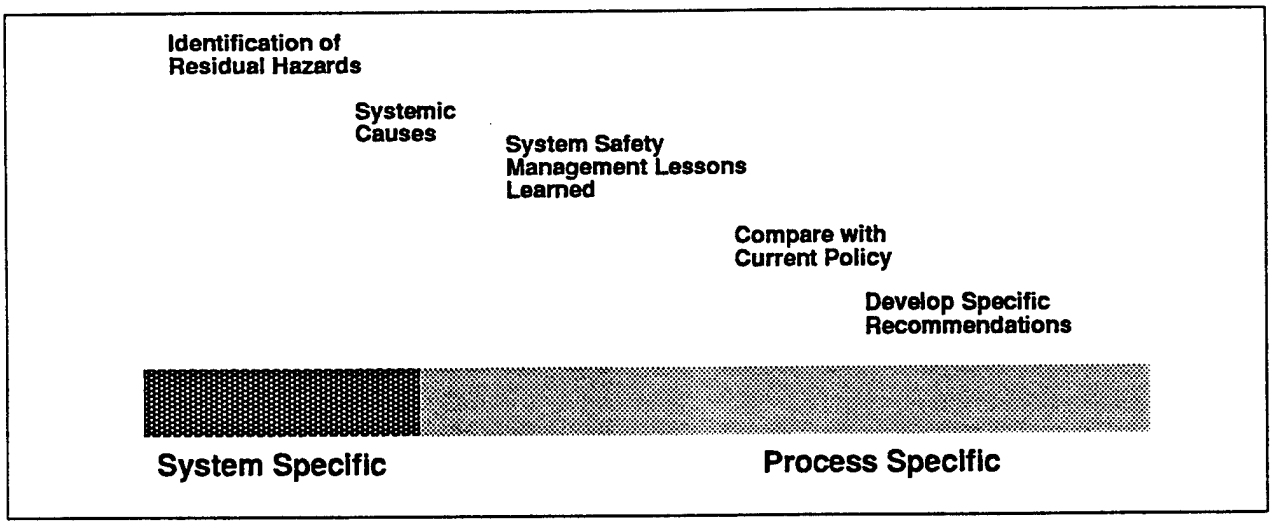

Figure 1. Process-Specific Orientation of the Study

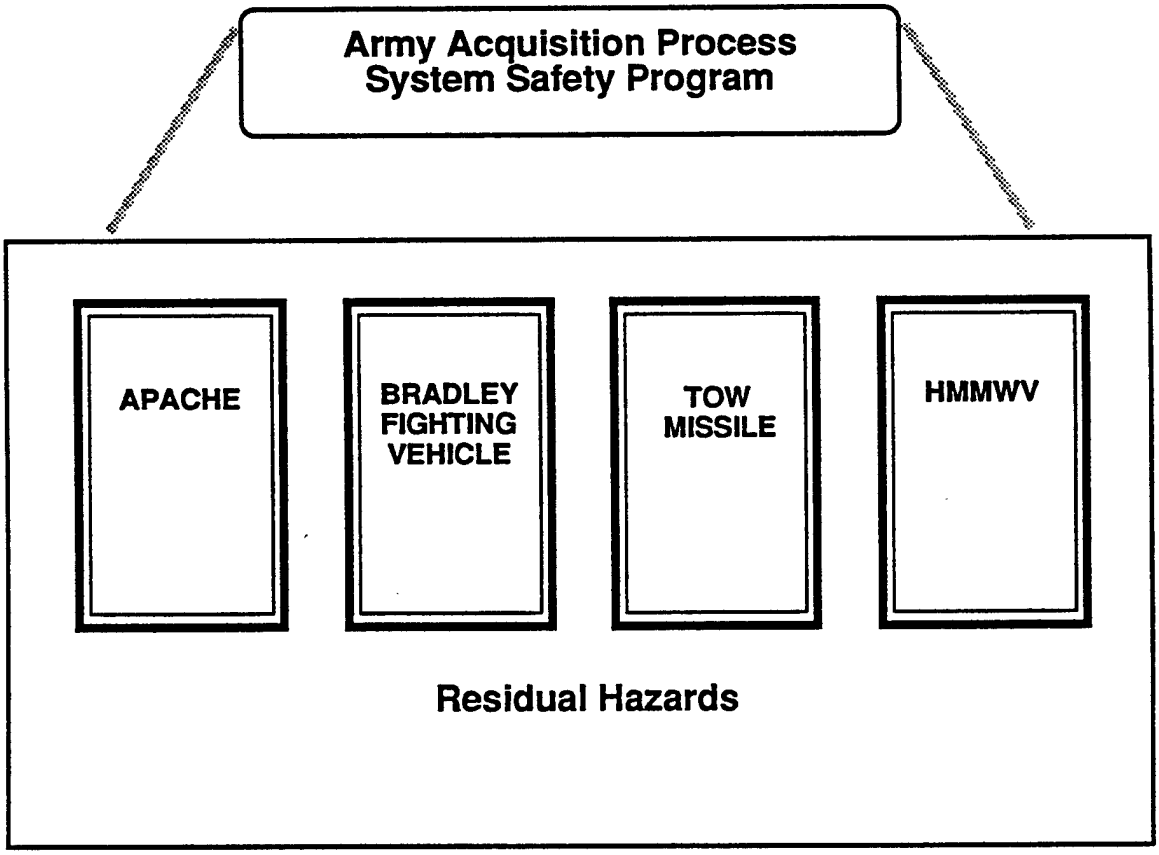

Figure 2. Systems Used as Windows on the Acquisition Process

programs and have had sufficient field exposure to have experienced mishaps. These selected systems provided windows on the acquisition process and the system safety program as a component part of that process. The objective was not to evaluate the safety of the selected systems.

The Bradley Fighting Vehicle System (BFV) is a fully tracked light combat vehicle with swimming capability. It has cross-country mobility compatible with the M1 Abrams main battle tank. Armament mounted on the two-man turret includes a stabilized 25mm automatic cannon with a coaxial 7.62 machine gun and a two-tube TOW missile launcher. There are two versions of the BFV which differ only in interior configuration: a nine man infantry version (M2) and a five-man cavalry version (M3).

The Apache is a twin-engine advanced attack helicopter with a fully articulated four-blade main rotor and a four-blade tail rotor mounted high on the port side of the tail pilon. It has tandem seats with the gunner/co-pilot forward of the pilot. Two cantilever wings aft of the pilot have hard-points to attach mixed ordnance or ferry tanks. A chain gun 30 mm automatic cannon is provided between the mainwheel legs.

The TOW missile is a tube launched, optically tracked, wire guided anti-armor missile. The basic ground launch TOW is composed of six components: a tripod mount, a traverse unit, the launch tube, an optical sight, a missile guidance set with battery assembly, and the encased missile. It has been the major armament on a number of helicopter and ground systems.

The High Mobility Multipurpose Wheeled Vehicle (HMMWV) is a 1-1/4 ton payload, diesel powered, high mobility 4x4 tactical wheeled vehicle with a common chassis and six body configurations to accommodate various ground transportation requirements. The various HMMWV versions are designed to serve in combat, combat support, and combat service support roles.

This study was necessarily limited by the systems that were used as examples of the acquisition process. However, systemic causal factors that were identified from this sampling of systems are expected to be generally applicable, since Army acquisition and system safety management practices stem from common policy documents. No nondevelopmental items or in-house developed systems were included in this study.

These systems were all developed prior to implementation of the Manpower and Personnel Integration (MANPRINT) program and the reorganization that placed all Program Managers (PMs) and Program Executive Officers (PEOs) under an Army Acquisition Executive. The impact of these programs was assessed by determining the degree to which their respective policies address system safety management lessons learned. This assessment was supplemented by discussions with MANPRINT, system safety and PMO personnel.

This study did not address hazards associated with support facilities for the selected systems, since mishap data rarely included information regarding facility-related hazards.

1.3 The Report

Acquisition and system safety terms used in this report conform to standard Army definitions unless otherwise noted. The remainder of this report presents the methodology and results of the activities noted in Section 1.1 above. Section 2 describes the methodology for this study. Section 3 contains a compilation of the causes of residual hazards. Section 4 contains the system safety management lessons learned aggregated from the causes of residual hazards, together with recommendations. Army comments to the draft technical report are summarized in Section 5. Section 6 contains a matrix that compares the system safety management lessons learned with current regulatory guidance. This provides an indication of the progress that has been made in the system safety program and areas that need to be improved. Section 7 provides conclusions reached in this study.

2.0 Methodology

The methodology used for this study was to examine residual hazards of selected emerging systems and their preceding development effort. This process was essentially an extension of accident investigation since it began with mishap data and the system's field experience to obtain a composite picture of the nature of the system's residual hazards. However, the study was directed at determining causal factors associated with the acquisition process.

A graphic presentation of the methodology is shown in Figure 3. The first step was to identify residual hazards associated with the selected systems. Since it was impossible to track all residual hazards through the acquisition process, certain well-known, high visibility hazards were selected for detailed tracking. These residual hazards illustrate a variety of systemic problems. Systemic or process causes were identified for each residual hazard and analyzed to determine why they exist. System safety management lessons learned were developed to address related systemic causes of residual hazards.

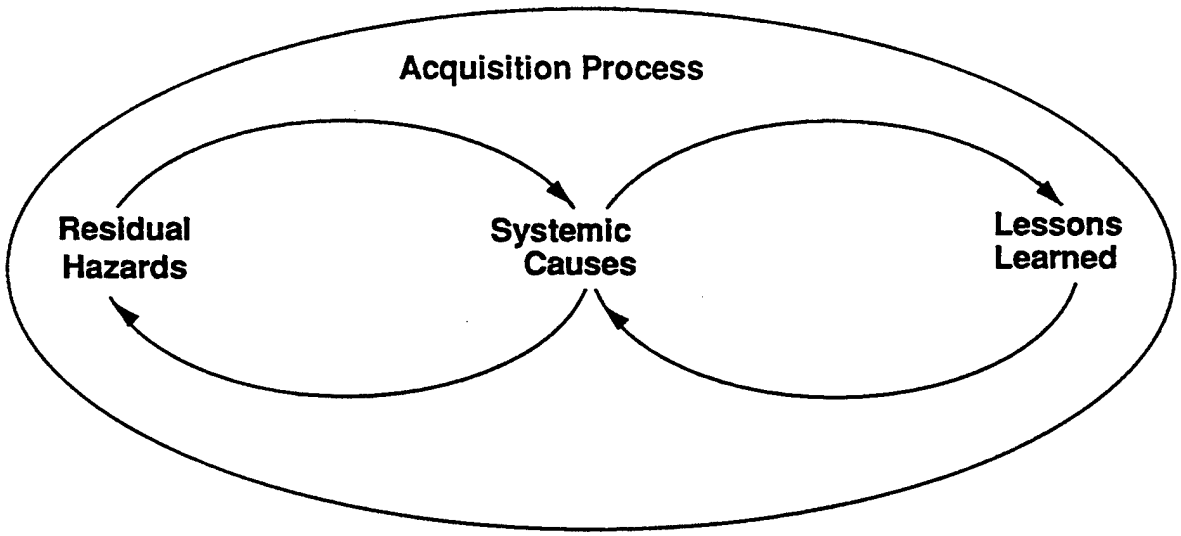

Figure 3. Process for Developing System Safety Management Lessons Learned

2.1 Identification of Residual Hazards

The hazard identification process involved several sources of information, as shown in Figure 4. Each source identified some of the residual hazards and provided a different perspective on the nature and significance of the residual hazards. Each source by itself was an incomplete picture of the full set of residual hazards. For example, the PMO perspective might differ from the user perspective. Acquisition data might identify hazards not noted in the safety analyses.

Mishap data was obtained for each system from the USASC Army Safety Management Information System (ASMIS) data base. This included all mishap data (Classes A-E) available in the ASMIS system. The mishap data was analyzed to determine significant residual hazards for each system.

Category 1 Equipment Improvement Recommendations (EIRs) and Quality Deficiency Reports (QDRs) from the Deficiency Reporting System (DRS) data base maintained by the Army Materiel Command's (AMC) Materiel Readiness Support Activity (MRSA) were examined to obtain supporting and supplemental information on residual risks to that found in ASMIS. Category 2 data from the DRS data base was reviewed on one system (HMMWV) to determine if safety related information was restricted to category 1 reports. Safety relevant information not included in category 1 reports was found that supported other sources of hazards information.

Discussions with personnel from the PMO and supporting safety office and the initial review of system safety and acquisition documentation helped to clarify the nature of the residual hazards previously identified and point out

other residual hazards with no corresponding mishaps in the ASMIS data base.

Residual hazards and associated system safety issues were discussed with system safety personnel associated with each system from the PMOs, contractors, AMC MSCs, AMC HQ, and DA. Other system safety, human factors and MANPRINT personnel provided input regarding generic system safety management issues. Visits were made to DoD, AMC HQ, the responsible PMOs and their respective supporting AMC MSC safety offices.

Discussions with system users also validated the residual hazards and identified further potential residual hazards. Field visits were made to Ft. Hood, Texas, and Ft. Lewis, Washington, to observe the selected systems and to talk to users and maintainers of these systems. This provided an opportunity to examine the systems and to obtain the users' perception of the residual hazards associated with the system. Apache trainers were also interviewed at Ft. Rucker. The following units provided support of this study:

Apache
Ft. Hood, Texas
- 1st Squadron, 6th Cavalry Brigade (Air Combat)
- 1st Battalion, 227 Aviation Regiment

Ft Rucker, Alabama
- Aviation Training Brigade

BFV
Ft. Hood, Texas
- 3rd Battalion, 41st Infantry Regiment, 2nd Armored Division
- 13th Battalion, 7th Infantry Regiment, 1st Cavalry Division

HMMWV
Ft. Lewis, Washington
- 2nd Battalion, 60th Infantry Regiment, 9th Infantry Division

TOW
Ft. Lewis, Washington
- 2nd Battalion, 60th Infantry Regiment, 9th Infantry Division

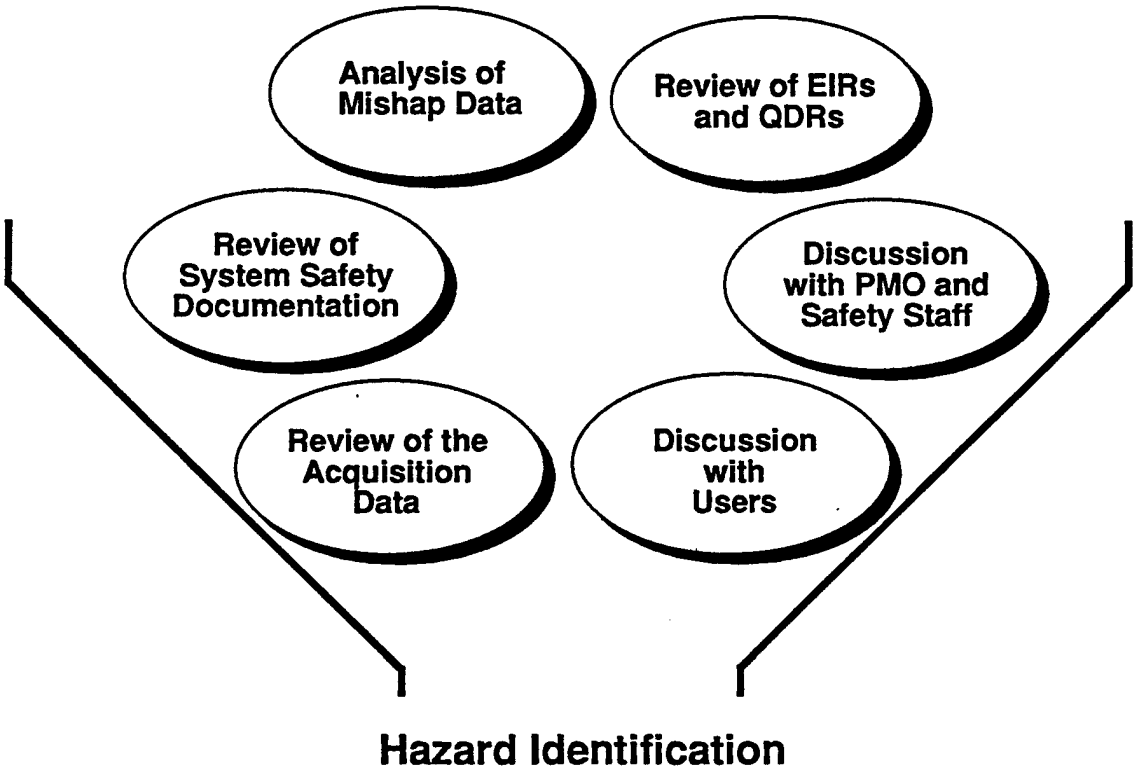

Figure 4. Hazard Identification Process

The local field safety offices were very supportive of this study and provided their own input on problems of tracking the field experience of these items for system safety purposes.

Two high-visibility residual hazards for each system were selected for detailed tracking throughout the acquisition process to provide objective examples to support the system safety management lessons learned. These residual hazards were selected after review of the mishap data, deficiency data, system safety analyses and acquisition documents; and discussions with Army and contractor system safety personnel, PM staff members and users. These hazards have received significant management attention and, in most cases, additional administrative or engineering control measures have been taken. Other residual hazards are also noted in this report where they help to illustrate specific systemic problems.

The following residual hazards were selected for tracking purposes:

Apache Helicopter

- The aircraft structure may not maintain a livable crewspace in a survivable crash.
- Inadvertent use of chop collar control during a critical flight phase may result in loss of the aircraft.

Bradley Fighting Vehicle

- Collapse of the trim vane during swimming may result in sinking of the BFV and potential injury or drowning of crew members.
- An individual in the turret basket doorway will be crushed if the turret rotates.

HMMWV

- The parking brake is adjustment sensitive. Misadjustment can result in vehicle damage from failure to hold on grade. Misadjustment of the parking brake or accumulation of mud and debris between the rotor and the brake can cause brake drag, with damage to the brake and adjacent fuel tank resulting in a loss of mobility.
- Vehicle rollover can result in vehicle damage and injury to occupants.

TOW Missile

- Stress corrosion cracking resulted in launch motor case ruptures.
- Delayed flight motor ignition resulted in premature detonation of the warhead or loss of missile guidance.

2.2 Systemic Causal Analysis

When an investigator asks why enough times, causes of a mishap may be traced, in part, back to the acquisition process. This study focuses on the systemic causes of mishaps and then examines why those causes exist.

For each residual hazard, it was necessary to determine the principal causal factor(s). A model of systemic sources of residual hazards in fielded systems is shown in Figure 5. Hazard communication is viewed as the mortar that binds the other system safety elements together into an effective

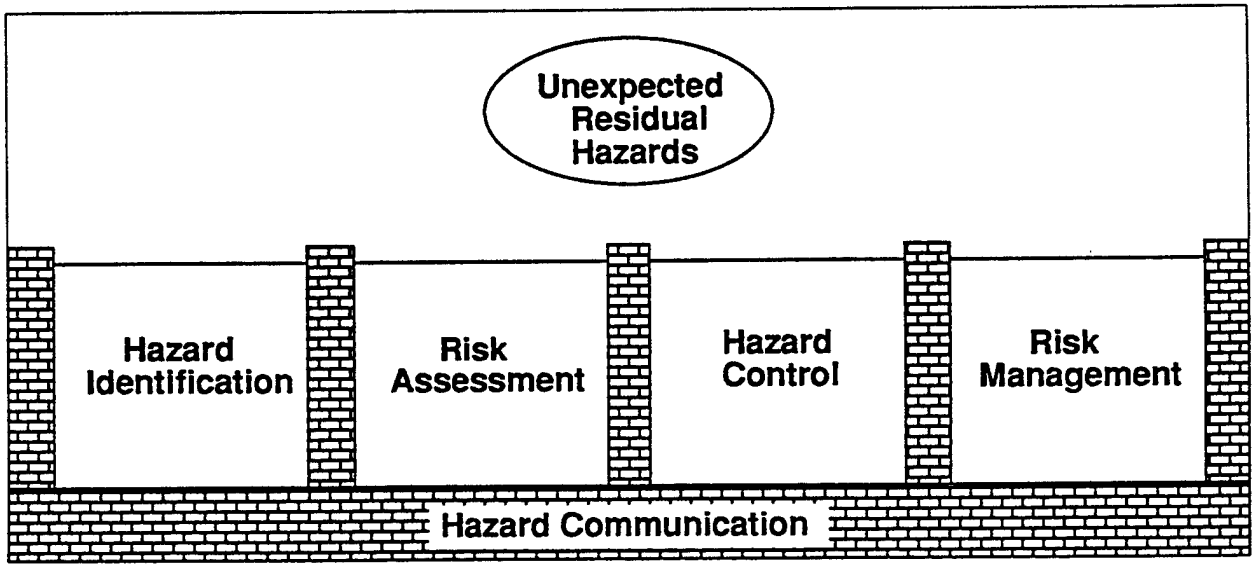

Figure 5. Systemic Sources of Residual Hazards

barrier to unexpected residual hazards. Unexpected residual hazards are those that were either never identified or the severity or frequency of resulting mishaps was not anticipated. Several basic questions were considered regarding residual hazards:

Identification: Were residual hazards that have since resulted in mishaps or potential mishaps identified during the acquisition process?

Assessment: Were the severity (consequences) and probability (frequency) of mishaps resulting from identified hazards expected?

Control: Were appropriate control measures taken and tested to verify their adequacy?

Risk Management: What was the basis for risk acceptance decisions, and at what level were they made?

Communication: Was sufficient hazard information available throughout the acquisition process for timely elimination or control of hazards?

The study was three dimensional, as shown in Figure 6. It involved tracking residual hazards of four systems through the acquisition process and asking the basic questions noted above. The Management Oversight and Risk Tree (MORT) logic diagram (Johnson 1973) was used as a logic check to ensure that all potential areas for lessons learned were examined at each phase of the acquisition process.

Answers to these fundamental questions helped to focus the analysis on specific portions of the acquisition documentation to identify causes of system safety management problems and successes.

System safety and acquisition documentation for each system was requested by USASC from the responsible PMOs. The requested documentation included:

- requirements documents
- system specifications
- safety design lessons learned from prior systems that were incorporated in the system design
- contractor analyses and Safety Assessment Reports (SARs)
- test and evaluation reports and Safety Releases
- Safety and Health Data Sheets
- system safety risk assessments
- decision packages and minutes from in-process reviews (IPRs) or Army Systems Acquisition Review Council (ASARC) meetings
- System operation and training manuals
- A listing of EIRs/QDRs
- A listing of system changes and improvements.

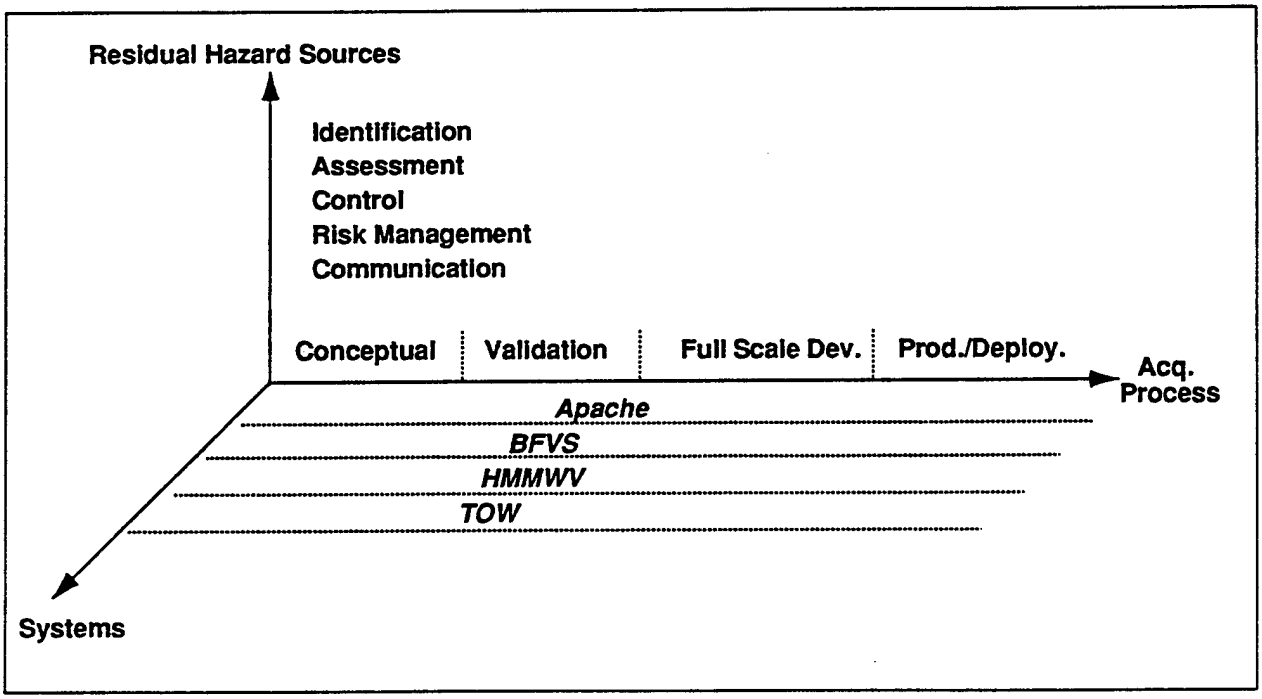

Figure 6. The Dimensions of the Development of Lessons Learned

The PMOs were unable to provide all information requested due to a variety of reasons, including lack of resources to find and copy the necessary documents and the absence of documents that were discarded when replaced by newer versions, discarded due to paper reduction programs or sent to records holding locations where they were not accessible. PNL researchers reviewed available documentation at the PMOs and supporting safety offices and copied as many relevant documents as possible during these visits. Documentation was also obtained through the Defense Technical Information Center and various other sources, including DA and AMC.

All system safety and acquisition documentation that could be obtained was reviewed to determine how specific residual hazards were identified, assessed, and resolved. Since the study included four systems and the focus was on the process rather than on individual systems, system safety management lessons learned are generally supported by two or more systems. The impact of incomplete documentation was not considered to be significant because of this redundancy.

2.3 Development of Lessons Learned

Systemic causes of mishaps were aggregated into system safety management lessons learned by considering related causes associated with specific parts of the acquisition process or systemic sources of residual hazards. This was also an iterative process (as depicted by the right loop in Figure 3). The lessons learned were refined as the interrelationships between causes became apparent.

The system safety management lessons learned were compared in a matrix with current policy documents to provide an indication of the current status of the Army's system safety program and to identify areas that could be improved. Specific recommendations are provided for individual policy documents as necessary in Appendix A.

Conclusions of this study are based on an overview of the systemic causes, the resulting lessons learned, and the implications of the lessons learned for improving the acquisition process.

3.0 Discussion of Causes of Residual Hazards

The crux of this study was to determine the causes of residual hazards. This central question has been stated in a variety of ways from differing perspectives. How do residual hazards get past the combat developer, the contractor, the materiel developer, the PM, the supporting safety office, technical testing, user testing and higher level decision makers? What is the cause of increasing safety restrictions on recently fielded equipment? Why do residual hazards occasionally come to Army decision makers' attention from the media rather than during the acquisition process? How can the Army system safety program do a better job of resolving hazards prior to fielding?

This section discusses the causes of residual hazards. These are presented by the systemic sources of residual hazards previously described in Section 2.2. It includes positive findings where an observed practice would improve the Army system safety program if uniformly implemented. It was necessary to understand these causes before lessons learned could be formulated.

3.1 Hazard Identification

The critical first step for system safety in the acquisition of new systems is hazard identification. Hazard identification requires a clear understanding of the tactical and peacetime use environment and the system performance requirements. Hazards are identified by analyses, review of predecessor and associated systems, study of new technologies and materials, and testing. Early involvement of system safety personnel is essential for timely identification of hazards.

The Army and the contractor both have important roles in hazard identification. The Army maintains hazard information on predecessor systems and establishes performance requirements and system safety program requirements necessary for hazard identification. The contractor analyzes hazards of the emerging design configuration based on the information and performance requirements provided. Both contractor and Army testing contribute to hazard identification. This section discusses systemic causes of residual hazards related to the hazard identification process.

3.1.1 Hazard Data on Past Systems

Requirements to consider historical safety data or lessons learned in the design of new systems flow down from DODI 5000.36. However, design lessons learned are not being systematically identified and compiled in a form that could be readily referenced in future contracts.

The selected systems had many opportunities for the use of historic safety data and lessons learned. The BFV grew out of the development efforts of the Mechanized Infantry Combat Vehicle (MICV), the Apache built on the development efforts on the Cheyenne, and the HMMWV grew out of the Expanded-Mobility Tactical Truck (EMTT) and the High Mobility Weapon Carrier (HMWC) programs. All three systems had opportunities for system safety lessons learned based on these prior development programs that had been terminated. These systems and the TOW also had fielded predecessor systems with the potential for safety lessons learned.

Examination of the HMMWV rollover hazard provides a positive example of the benefits of considering hazard data from predecessor systems. Even though consideration of past rollover lessons learned was not complete, the improved safety performance relative to the M151 rollover rate is significant.

In the examination of HMMWV acquisition data, there was evidence in the earliest documents that the rollover hazard with the M151, a HMMWV predecessor system, should be minimized. From CY 1983 to 1987, approximately one out of every 55 M151 in the field experienced a rollover accident during this five-year period with one fatality for every 21 rollover mishaps.

The Joint Mission Element Need Statement (JMENS) for the HMMWV[a] contained an assessment of existing systems. One deficiency of the M151 1/4 ton Jeep was

"mobility/agility (significantly degraded cross country)".

(a) Memorandum for the Secretary of the Army, W. Graham Clayton, Jr., Subject: Joint Mission Element Needs Statement (JMENS) for the High Mobility Multipurpose Wheeled Vehicle (HMMWV), 8 July 1980.

The HMMWV Independent Evaluation Plan[a] noted,

"While the 'common chassis' concept is not new, the idea of using a 'common chassis' for a high performance off-road and a high performance on-road machine is both new and untried. The soft suspension, quick steering and high ground clearance needed for off-road mobility inevitably present oversteering and overturning tendencies during on-road travel."

The specification for the HMMWV[b] stated in the safety section that

"suitable rollover protection shall be provided which shall be consistent with vehicle application, i.e. high speed off-road usage."

This requirement deals with mitigation of the consequences of rollover, but it does not provide a safety performance requirement, such as a high-speed emergency avoidance test, that would ensure that the actual rollover hazard was adequately resolved. The closest that the specification came to addressing the rollover issue was a requirement on turning:

"The vehicle shall be capable of sustaining from 0.4 to 0.6g lateral acceleration in a constant radius turn."

Moment equations using data on the M151 indicate that it would also meet this requirement. The ratios of the height of the center of gravity for the loaded vehicle to the track width for the HMMWV and the M151 are approximately equal.

Since fielding in CY 1983 through CY 1987, one HMMWV rollover was reported for about every 500 HMMWVs in the field during this period with no fatalities. Thus, the HMMWV design does appear to have reduced the probability of rollover accidents compared to the M151 by an order of magnitude. This may be somewhat optimistic, because interviews with field safety personnel indicate that many HMMWV rollover accidents may go unreported if there are no serious injuries and damage costs can be kept within the $1000 damage reportability criterion, whereas M151 rollover accidents tend to be reported due to injuries.

The HMMWV rollover hazard example shows that where lessons learned are considered in the design of new systems, mishap risks can be reduced. However, it also shows the need to translate lessons learned into safety performance specifications for new systems.

3.1.2 Hazards Associated with New Technologies

The Army has no system to collect and record hazards information associated with new technologies and materials. Failure to record such information and keep it up to date can lead to oversights in hazard recognition.

The TOW missile design was reported to have used the best materials and latest technology available at the time. The TOW missile Safety Statement[c] contained a launch motor failure mode and effects analysis that identified corrosion as a potential hazard leading to case failure. The probability of corrosion causing such failures was judged to be "very low," because the interior was sealed by the igniter and the exterior had a phosphate coating. Four launch motor ruptures occurred: two in 1980 involving foreign sales and two in 1986 at the Yakima Firing Range and Oahu. While details of the 1980 incidents were not available to the Missile Command (MICOM), a TOW failure investigation team was assembled to investigate the 1986 failures. The investigation report[d] concluded that stress corrosion cracking was the cause of these incidents. The report stated,

"it is well known that C-300 maraging steel is susceptible to stress corrosion cracking, especially when cold worked and aged to a tensile strength above 300 KSI (2,068 MPa)."

Stress corrosion cracking involves the combined action of stress and a mild corrosive environment, neither of which would cause concern by itself. This phenomenon was first extensively studied in relation to the failure of brass cartridge cases. At the time of the development of the TOW, it was known that certain maraging steels were susceptible to stress corrosion cracking when chlorides

---

(a) *Independent Evaluation Plan for the High Mobility Multipurpose Wheeled Vehicle (HMMWV)*, U.S. Army Materiel Systems Analysis Activity, Aberdeen Proving Ground, MD, June 1981.

(b) DAAEO7-83-C-R034 AM General Corporation, *System Specification High Mobility Multipurpose Wheeled Vehicle (HMMWV)*, U.S. Army Tank-Automotive Command, Warren, MI, February 1983.

(c) Dichter, H.S., *Engineering/Service Test Safety Statement Tow Heavy Assault Weapon, Report No. TOW-T20*, DA-01-021-AMC-13626(Z), Hughes Aircraft Company, Culver City, California, July 1966.

(d) Sanders, Sandra L., *Investigation of 1986 Yakima and Oahu TOW Launch Motor Failures*, Vol. 1, Technical Report RD-PR-87-7, U.S. Army Missile Command, Redstone Arsenal, AL, October 1987.

were present (Logan, 1967). Retrofit costs and programmatic impacts could have been avoided had this information been considered in the TOW development.

Army safety requirements don't always reflect improvements that should be expected from new technologies and materials. In a survivable crash, aircraft design provides a cushion that reduces the acceleration loads on the occupants to within human tolerance limits. Crash survivability requirements for the Apache were based on the 95th percentile potentially survivable crash of predecessor helicopters expressed in terms of impact velocities. These requirements, which have been incorporated into MIL-STD-1290, have not been upgraded to reflect technology improvements that could increase the cushioning effect of the design. When Army expectations as expressed in safety design standards do not keep pace with technology, both the severity and probability of mishaps may be excessive.

3.1.3 Consideration of Human Error

The potential for operator or user error is not receiving adequate attention as a source of system hazards in the design of new systems.

The majority of Army mishaps include human error as a primary or contributing cause. For each year from FY 1982 through FY 1987, human error was cited as a cause in 78 to 91 percent of the Class A aviation accidents (USASC, 1988).

Following the sinking of a BFV in 1987, the Army Chief of Staff suspended swim operations until a "positive lock" mechanism could be provided to prevent inadvertent collapse of the trim vane. In his message he stated,

"It is apparent that operator error in barrier erection was the proximate cause of the sinking. After personally reviewing the incident at Ft. Benning, I am convinced that procedures for erection of the trim vane mechanism leave too much potential for operator error. The safety of our soldiers compels us to eliminate this potential." [a]

This message reported that seven sinkings had been documented of which six were attributed to trim vane collapse. A subsequent Safety Assessment Report[b] from the contractor stated,

"To improve soldier reliability in trim vane erection, the spring-equipped turnbuckle system is being modified to a solid link support."

3.1.4 Understanding the Operational and Tactical Environment

Contractors and Army system safety personnel do not always have a clear understanding of how the system will be used in the tactical environment and may overlook operational hazards.

The contractor must have a clear understanding of how a system will be used to design the safest system possible. Hazards to HMMWV gunners might have been better controlled if designers had had a better understanding of the use environment. It is common practice to have gunners maintain a watch from their weapon station during operations. The use of these "air guards" on HMMWV TOW carriers seemed to come as a surprise to the collateral safety officer in the PMO who indicated that the HMMWV safety release did not permit this practice. A Test and Evaluation Command (TECOM) Safety Release[c] required all HMMWV TOW crew members to wear seat belts any time the vehicle was moving. However, the Operational Test and Evaluation Agency (OTEA) had objected stating that this requirement

"does not allow for realistic crew operations in a tactical environment"

and requested that this constraint be relaxed to permit some limited testing with the gunner in the turret while the vehicle was in motion.[d] This was permitted, but there was no apparent follow-up to provide increased protection for exposed gunners. TM 9-2320-280-10 under TOW weapon station operation, now advises the use of the gunner's sling as a seat rest or restraint if the gunner is positioned in the weapon station during travel. The use of the air guard is shown in training videos used at Ft. Lewis and was observed to be standard practice. Lack of understanding of user practices can thus have an impact on the safety of fielded systems. The gunner is unprotected in case of vehicle collision or rollover.

(a) Message, DALO-SMT, (General J. A. Wickham, Jr., CSA), Temporary Suspension of Bradley (M2/M3) Swim Operations, April 1987.

(b) *Bradley Fighting Vehicle Basic M2/M3 Safety Assessment Report, Contract DAAE07-86-C-R128*, FMV Corporation, Ordnance Division, San Jose, CA, May 1987.

(c) Message, TECOM, DRSTE-CM-R, 251920Z, Automotive Safety Release for the High Mobility Multipurpose Wheeled Vehicle (HMMWV), May 1982.

(d) Message, OTEA, CSTE-POO, 111630Z, Automotive Safety Release for the High Mobility Multipurpose Wheeled Vehicle (HMMWV), June 1982.

Ft. Lewis safety personnel also reported that they were considering issuing hockey masks to gunners. This was in response to numerous incidents where the gunner's face struck the weapon as the HMMWV driver pulled up to the firing point and quickly applied the brakes.

Most Army system safety personnel are located in the Major Subordinate Commands (MSCs) of the Army Materiel Command (AMC) and have limited user contact. They often have no military experience or other hands-on experience with the systems that they support. Due to the lack of qualified system safety engineers in the Training and Doctrine Command (TRADOC), safety input to requirements documents has been provided by system safety engineers at AMC.

Most requirements documents are limited in length and cannot contain the level of detail that is necessary to adequately address all safety performance requirements. Even though TRADOC sends out Required Operational Capability (ROC) statements to users for comment, user command safety offices do not see all ROCs and do not feel confident that their comments will be included in the ROC or subsequent requirements documents.

Where applicable, national consensus standards and regulatory safety requirements are used in specifications. The HMMWV specification stated that the HMMWV had to meet applicable requirements of MIL-STD-1180 for Type 1 vehicles. This standard cites specific requirements of the Federal Motor Vehicle Safety Standards. Such standards do not consider the military use environment and therefore cannot be referenced without qualifications and additions.

3.1.5 System Safety Input to Requirements Documents

Adequate safety performance requirements are not incorporated into requirements documents for new systems. The Army has not used this opportunity to prevent recurrence of past hazards to full advantage.

As noted in Section 3.1.1, design guidance resulting from technical safety lessons learned is not systematically gathered and stated as performance requirements that can be referenced in requirements documents.

In the history of armored vehicles, effective hatch retention mechanisms are a fairly recent development. This points to the need for translating historical lessons learned into safety performance requirements in requirements documents. A Tank-Automotive Command (TACOM) analysis of M113 Armored Personnel Carrier accidents from October 1981 through March 1985 showed that 56 of the 204 mishaps involved inadvertent closing of hatches and were design related.[a] Specifications for the BFV hatches resulted in an improved design. From CY 1982 to CY 1987, only 5 of 186 BFV mishaps involved inadvertent hatch closure. Only two of these were attributed to material failure.

The contractor must have a clear understanding of the Army's safety expectations for the proposed system. Such expectations are most clearly understood when they are expressed in terms of performance requirements coupled with the test methodology that will be used to evaluate safety performance. The HMMWV specification did not require rollover protection to pass any specific testing. As a result, no specific physical testing of rollover protection was conducted on initial HMMWVs. Recent tests on the roll cage over the cargo compartment of the HMMWV Interim Squad Carrier (ISC) have used the SAE J374 Roof Crush Test Procedure (SAE 1984). The HMMWV ISC was requested and funded by the 9th Infantry Division, Ft. Lewis, and required to protect troops transported in the cargo area of the ISC with a roll cage.

In a safety evaluation of the HMMWV conducted at Ft. Hunter-Liggett, California by the USASC,[b] it was noted that passengers could potentially be ejected from the troop area of the HMMWV troop carrier version since no individual restraint system was provided. The TACOM Safety Office commented,

"Unfortunately, the rear troop seating area is no better than the seating presently used in other Army systems. If meaningful protection is to be provided, the troop seating area has to be looked at as a system. Seats should be permanently attached (preferably facing the front of the vehicle) in accordance with Federal Motor Vehicle Safety Standard 207. Seat belts should be provided in accordance with FMVSS No. 208, 209, and 210. In addition, the passenger space should be protected by suitable rollover protection so that crew members in the rear area are provided the same degree of protection as those passengers in the presently permanently attached seats." [c]

(a) TACOM Safety Office, AMSTA-CZ, *Accident Report Analysis M113 Series Vehicles Alleged Material Defects FY81-1 April 1985*, U.S. Army Tank and Automotive Command, Warren, MI, June 1985.

(b) Letter, Subject: High Mobility Multipurpose Wheeled Vehicle (HMMWV), USASC, PESC-SE, 3 December 1984.

(c) Letter, Subject: High Mobility Multipurpose Wheeled Vehicle (HMMWV) Safety Concerns, TACOM, AMSTA-CZ with AMCPM-TVL concurrence, 18 January 1985.

These requirements, together with the SAE Roof Crush Test Procedure, should have been included in the specification. Instead, these vehicles were produced without passenger restraints or rollover protection in the troop seating area.

One measure of the effectiveness of the Army system safety program is the degree to which it influences the design of Army materiel to minimize residual risks of fielded systems. The closest that the Army system safety professional may ever get to designing a new system is in contributing to requirements and contractual documentation. The documentation flow builds on these initial documents; e.g., specifications and subsequent test and evaluation issues are based on initial requirements documents. Therefore, safety performance standards and system safety design criteria must be included from the beginning in the requirements documents for maximum effectiveness. Sweginnis (1987) points out the need for similar care in the system safety portions of RFPs. Unfortunately, early safety input too often includes only boilerplate statements that do not capture lessons learned. For example, the RFP for phase I of the BFVS Block II Modification[a] stated,

"The vehicle modifications to be developed under this contract shall comply with applicable human factors engineering, safety and health design, performance and operational requirements and not present uncontrolled safety and health hazards to personnel throughout the life cycle of the system."

This general statement is necessary but may not be sufficient to focus designers' attention on specific issues, such as the impact of modifications on the swim capabilities of the BFV.

Safety requirements ultimately contribute to mission effectiveness and therefore have as much place in early requirements documents as reliability, maintainability or mission performance factors. In a battlefield scenario, a mishap has the same impact as losses due to enemy action. A BFV at the bottom of the river due to a mishap has the same impact as a mobility kill due to engine failure; both result in potential system loss and definite mission impact. Similarly, the loss of an Apache due to inadvertent use of the chop collar control at low altitude precludes accomplishment of the current and future missions, just as does a loss due to enemy fire. Therefore, system safety input into the earliest requirements documents is a strategic necessity.

The TRADOC centers and schools produce most of the initial requirements documents. While there are other combat developers, TRADOC is the major combat developer in the Army. Until recently, there have been no trained system safety personnel in the TRADOC centers and schools to ensure that technical safety lessons learned were gathered and incorporated into initial requirements documents. Now, several entry-level safety engineering positions have been filled at a few of the centers and schools.

3.1.6 Testing Limitations in Hazard Identification

Testing is limited by availability of resources and may not be rigorous enough to detect specific hazards.

The final development test report of the BFV[b] stated,

"Insufficient developmental testing has been accomplished in various areas including...floating and swimming, due to time constraints."

The vehicle swim capability was tested in calm water with no current. This time constraint was partially imposed by Congress when, in 1977, it directed in public law that first production of the BFVS would take place by May 1981.

An Apache special task force report on technical and safety issues noted,

"There are numerous components on the AH-64 that have not had the qualification effort completed during the Phase II stage (Engineering Development). Many of these qualification efforts were deferred to be demonstrated and substantiated in preproduction testing and the First Article Test. In general, many of the components require issues to be resolved or testing to be completed." [c]

Time, funding and sample limitations mean that certain low probability or time-dependent hazards may not be observed during testing. The TOW missile launch motor case rupture hazard involved stress corrosion cracking, which did not result in mishaps until years after fielding.

Test directors and test personnel have not had adequate system safety training, and system safety personnel do not usually have direct involvement in testing, as do human

(a) RFP DAAEO7-85-R-R023, BFVS Block II Modification, Phase I, 1985.

(b) *Final Report Development Test IIA (DTIIA) of Infantry Fighting Vehicle and Calvary Fighting Vehicle*, TECOM Project 1-VC-030-IFV-007, Aberdeen Proving Ground, MD, February 1981.

(c) *Apache Special Task Force Technical and Safety Issues*, November 1987.

factors engineers. During the operational testing of the HMMWV, there were several test incidents. Some of these were attributed to operator error and some were defined as "operational mission failures." The report states,

"Candidate HMMWVs and baseline vehicles were involved in accidents during the operational testing. Of major significance is that no serious injuries resulted from these accidents. Material damage varied from major to minor. In most cases, the exact cause of the incident could not be determined. While undoubtedly some number of the accidents were caused by operator error, others were the result of the characteristics of the vehicle." [a]

The independent evaluation of this operational test noted that five of the nine incidents were considered major accidents including one 360° rollover.[b]

Testing is expensive, and it is necessary to maximize the data obtained during testing. User testing is the closest approximation to field use available while the contractor is still responsible for the design. This is a strategic opportunity for verification of system safety in the use environment. System safety trained user test personnel, or qualified system safety engineering support for observation of operational tests and investigation of test incidents might have yielded more useful data related to the adequacy of the HMMWV design.

The Combat Systems Test Activity (CSTA) reports that it has a contractor providing system safety training for test engineers. Such training is relatively new and not available to all TECOM sites or to user test directors. The system safety engineer is available to help support CSTA test directors.

Army system safety personnel are not usually involved in engineering or user testing. A directive for USASC involvement with HMMWV testing noted that the Army Vice Chief of Staff upon reading about a HMMWV driveshaft problem, said,

"This is why the USASC needs to be in early on system developments."

The USASC observed HMMWV user testing at the Combat Developments and Experimentation Command, Ft. Hunter-Liggett, California. This was the first time that any qualified system safety personnel had been directly involved in HMMWV testing. Some of the hazards noted by USASC had not been previously identified.

3.1.7 Fielded Systems

System safety personnel do not participate in post-fielding system reviews of ground systems at user sites.

The principal means of user feedback on system hazards are Mishap Reports, Quality Deficiency Reports (QDRs) and Equipment Improvement Reports (EIRs). For the selected systems, these reports were not used to report "near misses or close calls." One safety office reported that they had some success in obtaining such information from Logistics Assistance Office reports from user sites.

The field visits conducted in conjunction with this study revealed new potential hazards and provided a better understanding of the nature of previously identified hazards (see Sections 3.3.2 and 3.3.6).

3.2 Risk Assessment

Risk is a measure of possible loss in terms of the severity and probability of a hazard. Risk assessment is conducted by contractors, testers and Army system safety personnel supporting the PMOs. Risk assessment is the process of estimating the severity and probability for each identified hazard. Hazard severity can usually be accurately predicted. Prediction of hazard probability, however, is more difficult. This section addresses problems in estimating and interpreting hazard probability that may contribute to errors in risk acceptance and thus lead to higher mishap rates than expected for residual hazards.

3.2.1 Estimating Human Reliability/Human Error Rates

Risk assessments often involve overly optimistic reductions in hazard probability attributed to human performance.

One problem in estimating hazard probability is the lack of any method for predicting human reliability or, conversely, human error. No standardized method of predicting human reliability such, as that described by Bell and Swain (1985), has been adopted to reduce errors in assessing hazard probabilities involving human performance.

(a) *High Mobility Multipurpose Wheeled Vehicle U.S. Army-U.S. Marine Corps Operational Test II*, OTEA, Falls Church, VA, January 1983.

(b) *Independent Evaluation of the High Mobility Multipurpose Wheeled Vehicle (HMMWV) Operational Test II (OT II)*, OTEA, Falls Church, VA, March 1984.

The HMMWV rollover probability without control measures was described as "occasional" in the HMMWV production Safety Assessment Report.[a] With

"proper crew training, familiarity with vehicle characteristics and compliance to MIL-STD-1180"

the hazard probability was reassessed as "improbable," which for the HMMWV fleet would mean that rollover was "unlikely to occur, but possible." MIL-STD-1180 does not deal with roll stability but does address rollover protection and seatbelts. Conformance with this standard would reduce only the severity of a mishap. Therefore, the reduction in hazard probability due to the control measures listed is strictly user-dependent. The 26 rollovers reported from fielding in CY 1983 through CY 1987 show that rollovers across the HMMWV fleet have occurred "several times" and that either the original hazard probability of "occasional" was correct or the assumptions regarding training were incorrect.

Design of the Apache chop collar control also failed to take adequate consideration of the potential for human error. The Apache System Hazard Analysis Report[b] rated the hazard severity as critical and the probability of the inadvertent activation of the chop collar at the lowest level (see 3.3.4).

3.2.2 Consideration of Exposure

Exposure is not usually considered in the risk assessment process.

Risk assessment cannot be properly interpreted without considering exposure. MIL-STD-882 hazard classification guidance only indirectly accounts for exposure in terms of the life expectancy of the item or inventory. It does not address exposure in considering users or time-dependent events.

The BFV turret shield door crushing hazard was assessed as having a remote probability; i.e., "unlikely but possible to occur in the life of an item." The low assessment of probability could lead one to accept the risk associated with this hazard if there was no consideration of exposure. Given that production of the BFV began in May 1981 and reached 2900 vehicles in April 1988, one can conservatively estimate potential exposure at over 14,000,000 passages of crew members through this doorway over this period. To be caught in the doorway requires that an individual is in the doorway when the turret is rotated. That individual must have failed to ensure that the turret power was off and failed to engage the turret lock. The contractor had reported that their test operators had failed to engage the turret lock prior to exiting the turret.[c] Further, personnel entering the turret could not readily determine whether turret power was on or if the turret travel lock was engaged. The A1 version included turret drive warning lights at the doorway visible to those entering the turret. Even a probability of one such incident in a million could therefore result in 14 door-crushing mishaps. Mishap data contained 14 incidents through August 1987. The PMO authorized investigation of a turret door interlock in April 1987 after a soldier was pinned in a BFV turret door in Germany. This indicates that a low probability of occurrence is not sufficient justification to accept a hazard; exposure must also be considered.

This example also shows that examination of exposure can highlight areas where human performance and human error rate considerations impact risk. The overreliance on human performance in hazard control (see Section 3.3.5) emphasizes the need to consider exposure in addition to the risk matrix shown in MIL-STD-882B.

Consideration of exposure is standard practice in the assessment of health hazards involving toxic chemicals or physical agents, such as noise. There is obviously no risk if there is no exposure, regardless of the concentration of a toxic chemical, the intensity of a physical agent, or the probability that they will be present.

The exposure factor is also useful in considering time-dependent events or the simultaneous occurrence of events. The HMMWV fuel tank has a drain plug that can be pulled out like a rubber stopper. This event, reported in category 2 EIR/QDRs, has not resulted in any fires or system damage. In this case, the hazard exposure factor could be the probability that a source of ignition will be present.

3.2.3 Hazard Probability - Getting Down to the Numbers

MIL-STD-882 definitions of hazard probability and its qualitative hazard probability categories are ambiguous.

MIL-STD-882 is the basis for risk level definition and determination by both contractor and Army system safety personnel.

(a) *Safety Assessment Report (Final) (HMMWV Production), Contract DAAE07-83-C-R034*, LTV Aerospace and Defense Co. AM General Division, Livonia, MI, August 1984.

(b) Jacobs, R.L., *System Hazard Analysis Report, Report No. 77-HA-8004, DAAJ01-77-C-0064*, Hughes Helicopters, June 1975.

(c) *Bradley Fighting Vehicle Safety Statement, Contract DAAK 30-80-C-0022, DI-H-1322A*, FMC Corp, Ordnance Division, San Jose, CA, December 1981.

The definition of hazard probability in MIL-STD-882 is inconsistent. It describes hazard probability as "the aggregate probability of occurrence of the individual hazardous events that create a specific hazard." It later describes hazard probability as a rate. Unfortunately, the qualitative hazard probability categories provided in the example are based on the expected life of the system or fleet rather than on the measures of use.

Hazard probability category definitions may be tailored to program objectives as long as the contractor and the PM concur. However, the qualitative definitions for each level in the example in MIL-STD-882 are usually adopted verbatim by contractors and the Army. This standard provides no equivalent quantitative example of hazard probability categories.

In the qualitative example, hazard probability definitions for both the item and the fleet or inventory are confusing. There is no clear distinction between the definitions for occasional and remote hazard probabilities for the individual item, or between remote and improbable hazard probabilities at the fleet level.

Hazard probability categories often serve only as a relative ranking of hazards in the early stages of development. However, ambiguous definitions make it hard to question the hazard assessment and, worse, may result in a hazard being accepted when further corrective action might have been warranted.

The only system in this study where the contractor used quantitative hazard probabilities was the initial development of the TOW missile. Component and subsystem reliability data were used, together with accumulated test data, to provide estimates of hazard probability.

At some point in the development of any major system, the acquisition decision maker must get down to the numbers to estimate the projected losses that can be expected if a given hazard is accepted. However, the qualitative assessment developed by the contractor is not often converted to a quantitative assessment. This is usually true even after the system is fielded and actual rates can be calculated. The one exception noted in this study was that the PMO has calculated the hazard probability rates for the three major residual hazards of the TOW missile.

3.3 Hazard Control and Evaluation of Control Measures

Control of hazards involves the selection and evaluation of control measures. This section discusses causes of residual hazards associated with the hazard control process.

3.3.1 System Safety Design Guidance

System safety design guidelines have not been recorded in a format that can be referenced in specifications and made available to contractor designers and system safety personnel.

When system safety design guidelines are only kept in the Army's institutional memory, they are easily lost or overlooked. They are not available to contractors designing new systems. User comments regarding system hazards during this study often pointed to prior system designs that eliminated or controlled the problem.

One contractor indicated that they maintain their own data base of safety design lessons learned. This indicates that there may be barriers in both directions: the Army may not benefit from safety design guidance developed by the contractor.

There is a lack of appropriate safety standards or handbooks available to provide guidance for the design of Army materiel. There is limited system safety design guidance contained in the Tri-Service human factors MIL-STD-1472 and MIL-HDBK-759, but this guidance is insufficient for Army systems.

An Army system safety design handbook was proposed in 1978, with one objective being to

"act as a focal point for safety engineering design feedback from developers, testers, manufacturers, and the field." [a]

This proposed handbook has since been divided into a general system safety handbook and a series of commodity-specific safety design handbooks. Only one of these handbooks is reported to have been issued to date.

3.3.2 Early User Review of Proposed Hazard Control Measures

There was inadequate early user involvement in review of system hazards and proposed control measures.

User involvement tended to come during testing when the design was fixed. The HMMWV visibility problems iden-

(a) RFP 79-02-1686 under Government Prime Contract No. DAAG34-73-C-0051, Safety Engineering Design Guide for Army Materiel, 1979.

(b) Prost, Major W. A., *Independent Evaluation of the High Mobility Multipurpose Wheeled Vehicle (HMMWV) Operational Test II (OT II)*, IER-OT-054, OTEA, CSTE-ED, Falls Church, VA, March 1984.

tified during testing could not be eliminated. The contractor was limited by the existing configuration in the modifications that could be made.

The double hearing protection requirement for the BFVS illustrates the need for user input in determining if control measures are realistic before they are adopted. Interviews with 43 BFV crew members revealed only one person who uses double hearing protection when the gun or vehicle is operated. Most crew members indicated that the use of double hearing protection interfered with communication. Double hearing protection was considered unacceptable for use by troops in regard to requirements for the TOW/HMMWV gunner.[b] Such input could change the entire risk picture (see 3.5.4). Early user input on lack of protection of HMWWV "air guards" in a collision or rollover might also have resulted in a better design.

3.3.3 Validation of Control Measures for Known Hazards

There is no specific requirement to verify that the control measures for severe (critical or catastrophic) hazards are validated during testing.

Most residual hazards were identified prior to testing. However, their control measures may not have been specifically verified. Tests criteria are based on the Required Operational Capability (ROC) or performance requirements in the specifications, which often do not include adequate safety performance requirements.

Hazard information provided in Safety Assessment Reports (SARs, previously called Safety Statements) has been used to ensure safety of test personnel. It has not been routinely used as a basis for test planning to ensure that systems are safe.

Technical safety testing is conducted to identify and evaluate hazards associated with the systems being tested. The principal system safety Test Operations Procedure (TOP)[a] contains no requirement to systematically verify the adequacy of hazard control measures for severe hazards identified in contractor hazard analyses or in the SAR. The emphasis of this TOP is on inspections to identify residual hazards and safety subtests to evaluate safety criteria from requirements documents.

User-dependent control measures are verified to the extent that the user is not injured during testing. No test personnel were crushed in the turret shield door during testing of the BFV, but the adequacy of the control measures to prevent such incidents was never verified, even though this was identified as a severe hazard.

3.3.4 Compliance with Standards

Contractor compliance with standards may be erroneously interpreted as proof of meeting specific system safety criteria.

Compliance with standards is not sufficient evidence to judge that control measures are adequate.

A principal cause of the Apache chop collar hazard (see 3.3.5) was failure to validate the adequacy of the control measures. The use of a detent was one method prescribed in MIL-STD-1472 for prevention of accidental activation of controls. The Apache System Hazard Analysis Report[b] rated the hazard severity as critical and the probability of the inadvertent activation of the chop collar at the lowest level. The contractor later concluded,[c]

"The engine cut switch is designed to be unique to prevent inadvertent engine cut. The hazard is eliminated by design."

No testing was completed to evaluate the adequacy of this control measure or to determine if it was appropriate in this situation.

MIL-STD-1290 permits a contractor to evaluate the airframe's structural crashworthiness by analysis due to the high costs of destructive testing. However, there was no evidence that the methodology used for this analysis of the Apache crashworthiness was ever validated by the Army.

3.3.5 Overreliance on Human Performance in Hazard Control

There is an unnecessary reliance on user-dependent hazard control measures that could be eliminated by design.

Human performance was clearly an issue in half of the residual hazards selected for this study. It becomes a potential issue wherever administrative hazard control measures are used.

The Apache chop collar (see 3.1.4) and the BFV turret shield door hazards provided the clearest examples of

---

(a) *System Safety Engineering, Test Operations Procedure (TOP) 1-1-060*, TECOM, AMSTE-RP-702-100, Aberdeen Proving Ground, MD, April 1986.

(b) Jacobs, R.L., *System Hazard Analysis Report, Report No. 77-HA-8004, DAAJ01-77-C-0064*, Hughes Helicopters, June 1975.

(c) Jacobs, R.L., *System Safety Statement for the Phase 2 YAH-64 Advanced Attack Helicopter, Report No. 77-SS-0010, DAAJ01-77-C-0064*, Hughes Helicopters, December 1977.

design-preventable situations where performance-shaping factors, such as task loading or inadequate human engineering design, could predispose crew members to errors that could result in mishaps.

The December 1977 Apache System Safety Statement[a] identified the hazard as

"Loss of aircraft due to inadvertent engine cut during critical flight phase caused by similarity between the engine cut switch and friction devices on other aircraft."

It was noted that the Apache chop collar control, a knurled ring around the collective stick, closely resembles the collective friction control in the Huey and that

"the engine switch should be unique."

Rather than changing the location or design of this control, a detent was added that required the user to push the collar forward and then rotate it to chop or restore engine power. No human factors evaluation of this control was made to determine effectiveness of the detent in precluding inadvertent engine cut during normal operation of the collective. The hazard was clearly identified. The hazard probability, which reflects human error rates, was assessed at the lowest level. This hazard probability appears in retrospect to have been overly optimistic. Two aircraft have been destroyed and and four persons injured as a result of this residual hazard.

Following these incidents, a Safety of Flight message[b] was issued in August 1987 to alert users to the potential for inadvertent activation of the chop collar with supplemental information in the Technical Manual (TM) and to require that the chop collar be painted yellow to emphasize "the emergency nature of its function." A Maintenance Information message[c] was issued in February 1988 to provide advanced notice of an urgent Modification Work Order for installation of a break wire on both chop collar controls and to provide changes to TMs. These measures have reduced the hazard probability, but they have not eliminated the hazard. Since a pilot may operate a control by feel, painting the chop collar has not eliminated the potential for inadvertent activation. The use of break wire is also not a sure deterrent to human error. Further, the use of break wire may cause confusion or delay the proper operation of the chop collar in an emergency that requires its use. Pilot comments regarding the chop collar noted in Section 3.3.6 indicate a recognition of an error-prone situation, possibly from near-miss experiences.

The BFV safety statement[d] recognized the potential for occupants to be injured in the turret doorway when the turret turns if the travel lock has not been engaged and turret power turned off. A comment concerning validation of this procedural control in the safety statement indicates that

"Failures to lock due to human error have been noted when procedures were not followed."

The Army Human Factors Engineering Analysis[e] did not address the human error issue but did express concern over incomplete engagement of the turret lock. There were 14 Army mishaps in the ASMIS database through August 1987 involving individuals who had suffered crushing injuries in the turret shield door. FMC recorded 17 such mishaps through July 1988.

Too often, users are asked to compensate for hazards that could have been eliminated or controlled by design. This was evident in examining HMMWV visibility problems. In a Human Factors/Safety Assessment Report by the contractor on Dual-Net Communications Kits,[f] it was found that

"... drivers could eliminate or reduce the amount of vision obstruction through the right side windshield by shifting their head and upper torso forward and inboard (towards the radios). Using this procedure, the drivers were able to safely perform right hand turns while avoiding ground obstacles."

(a) Jacobs, R.L., *System Safety Statement for the Phase 2 YAH-64 Advanced Attack Helicopter, Report No. 77-SS-0010, DAAJ01-77-C-0064*, Hughes Helicopters, December 1977.

(b) Message, AVSCOM, AMSAV-XSOF, 201330Z, Safety-of-Flight Message, Operational, AH-64A Aircraft, Operation of Engine Chop Collar (AH-64-87-18) (TB 55-1520-238-20-23), August 1987.

(c) Message, AVSCOM, AMSAV-XSOF, 122000Z, Maintenance Information Message, AH-64 Aircraft, Advance Notice of MWO for the Modification of Engine Chop Collar (AH-64-88-MIM-02), February 1988.

(d) *Bradley Fighting Vehicle Safety Statement, Contract DAAK 30-80-C-0022, DI-H-1322A*, FMC Corp, Ordnance Division, San Jose, CA, December 1981.

(e) Human Factors Engineering Analysis (HFEA) for the Infantry Fighting Vehicle/Cavalry Fighting Vehicle (IFV/CFV), XM2/XM3, ASARC III, DRXHE-SP, U.S. Army Human Engineering Laboratory, Aberdeen Proving Ground, MD, 5 December 1979.

(f) Kunz, M.L., *Human Factors/Safety Assessment Report Dual-Net Communication System*, LTV Aerospace and Defense Co. AM General Division, Livonia, MI, June 1986.

This indicates that if the driver is aware of obstacles, adaptive behavior (peering around the radio equipment) can compensate for restricted visibility. Adaptive behavior may not compensate when the driver is not aware of obstacles, pedestrians or approaching vehicles in this blind spot. Several other visibility problems were noted with the HMMWV during development. Modifications to improve visibility were made, but they were limited by the existing design configuration. An April 1986 Safety of Use message notes,

"The small side mirrors of the HMMWV provide limited rearward vision. Drivers must be particularly alert when backing vehicles and rear ground guides must be used to the maximum extent possible."

Visibility was a primary or contributing factor in 26 HMMWV mishaps from December 1985 through February 1988.

3.3.6 Safety Evaluation Fielded System Performance

Army system safety personnel do not talk to users of recently fielded systems as a means of evaluating the adequacy of control measures and obtaining suggested control measures from the field.

Actual safety performance is not routinely compared to the expected risks from accepted residual hazards. The use of mishap reports to evaluate the safety performance of systems does not capture low-severity hazards due to reporting thresholds or information from near-miss incidents (see 3.5.5 for other limitations). Initiatives to study the highest injury-producing systems are a step in this direction, but this overlooks the comparison with the Army's expectations from the risk management process and comes after the injuries have occurred.

A questionnaire was given to Apache pilots at Ft. Hood asking them to list problems experienced or concerns regarding each preflight check area. In the 20 survey responses, several comments were made regarding the chop collar control:

"Often when reversing polarity, I worry about sliding my hand up on the chop collar."

"Chop collar is in a very dangerous location!"

"Not sure if a chop collar is necessary."

"Chop collar is bad!"

Such pilot inputs could be very useful in reducing residual hazards and in developing safety design lessons learned. For instance, 13 of 20 pilots expressed concern with the fuel management system, stating that certain combinations of switches could cause inadvertent engine failure due to fuel starvation. Most pilots thought the system cumbersome and error prone, requiring excessive attention for normal balanced flight. It is clear that the fuel management system must be simple, reliable and intuitive to operate to avoid such problems.

3.4 Risk Management

Risk management is the process of balancing the impacts of projected mishaps on resources, the acquisition program and mission against impacts of correcting the hazard on performance, cost and schedule. This recognizes that some residual hazards will be accepted because controls are infeasible, would degrade system performance, or are not cost effective. This section discusses problems that could lead to inappropriate decisions in the risk management process or failure to make decisions with resulting unexpected losses due to mishaps.

3.4.1 Limitations of the Risk-Management Process

Due to limitations in the risk-management process, no risk-management decisions are ever recorded for a significant portion of identified hazards.

The Army acquisition management system is a form of management by exception. Therefore, higher-level decision makers tend to be concerned only with hazards that could become "show stoppers." A hazard is not usually considered to be significant unless it has been noted during testing.

The Army test community classifies risks as deficiencies, shortcomings, suggested improvements or acceptable risks, based on definitions of these terms found in AR 310-25. TECOM uses these definitions in TOP 1-1-012[a] combined with the MIL-STD-882 risk matrix to classify risks, with deficiencies corresponding to high-risk levels on the matrix. The actual risk classification is reviewed and sometimes debated during the scoring conference. Hazards that have been classified as deficiencies by the test community will receive thorough review, since deficiencies are a bar to type classification. These high-risk hazards are elevated for Materiel Acquisition Decision Process (MADP) review, together with a "get well plan." However,

(a) *Classification of Deficiencies and Shortcomings*, TOP 1-1-012, with Change 3, TECOM, DRSTE-AD-M, Aberdeen Proving Ground, MD, December 1985.

shortcomings or suggested improvements reported in test reports are much less likely to be corrected, regardless of the cost involved. Thus, residual hazards may be accepted without further review by higher acquisition management or documentation of risk-acceptance decisions.

Risk-management decisions usually coincide with acquisition milestones. This tends to push risk decisions toward the end of the development phase, when there is less latitude for resolution due to financial and schedule constraints. The TACOM Safety Office recommended no materiel release of the HMMWV Group I utility vehicles in June 1985[a] because of a number of problems, including problems with the parking brake. It was recommended that in subsequent testing, the vehicle not be parked on slopes exceeding 20 percent because of brake test performance and the lack of a park position on the automatic transmission. This was contested by the PM, who argued that this was not supported by any other functional directorate or AMSAA and that a proposed preventive-maintenance proposal would control the identified brake failures. This solution caused the least interruption of schedule for this Tri-Service vehicle. Retrofit of some 37,000 HMMWV brake systems is now planned using the parking brake system found on Group II vehicles. There is some concern that this new parking brake may not eliminate all past brake problems because this brake, like those on Group I vehicles, has experienced brake drag and overheating problems resulting in warped rotors, glazed brake pads and melting of the adjacent main fuel tank.

3.4.2 Hazards that Bypass Risk-Management Decisions

There is no mechanism to ensure that risk management decisions are made at a level of acquisition management commensurate with the risk.

In this study, the terms acquisition management and decision makers include the PM and higher Army managers with decision authority for a given program.

While the supporting safety office uses all hazard information available, the hazards information passed on to higher level decision makers generally comes from test reports of technical, user, health hazard or human factors testing. Therefore the majority of hazard information initially generated by the contractor is never considered by higher decision makers. If the hazard isn't identified during testing (or later through field experience), it is not considered significant. As shown in Section 3.1.6, there are many ways that hazards can go undetected during testing. Therefore, significant residual hazards may never be identified to acquisition management.

Even though the BFV turret door crushing hazard was identified by the contractor and clearly described, it was never elevated to the PM or higher decision makers by the TACOM safety office, because no incidents were identified during testing.

The supporting safety office acts as the Army's principal risk- acceptance authority in its determination of hazards that are judged to require further resolution. The supporting safety office presents a safety position, rather than a statement of the risk and recommendations for the decision maker. When the user or the PM disagree with the safety office position, the risk-acceptance decision is passed on to acquisition management. For major systems, AMC headquarters may also disagree with the MSC safety office position, thus forcing the PM to take action or justify risk acceptance.

3.5 Communication of Hazards

Information on system hazards may be generated throughout the life cycle, from system concept to disposal. The following problems involve inadequacies in the collection and dissemination of such information.

3.5.1 Hazard Tracking

There is no all-purpose hazard tracking system used throughout the acquisition process.

The Army has not maintained hazard tracking systems for the selected systems. The USASC initiated a hazard tracking system for the Apache development but discontinued the effort due to lack of resources required to maintain this data base. It is apparent that contractors have tracked hazards at various points during system acquisition, but it is not evident that this has been a consistent effort. Early hazard analyses identify system hazards that may be used as the basis for a tracking system. Without such a system, it is difficult to determine what risk management decisions were made and what the expected risk had been at the point when the decisions were made.

3.5.2 Unique Identification of Hazards

When hazards are tracked by contractors, they are not always uniquely identified.

This was noted in tracking the chop collar hazard for the Apache. The first mention of the chop collar is in a hazard

(a) Jarvis, G.G., Certificate of Materiel Release (HMMWV Utility Vehicles), TACOM, AMSTA-CZ, 19 June 1985.

report in the Apache System Hazard Analysis of June, 1975.[a] The chop collar was identified as a hazard (No. 703011), even though the nature of the hazard and corrective action are somewhat unclear. The System Safety Statement of December 1977[b] makes a clear and concise statement of the hazard of inadvertent chop collar actuation. The hazard description (No. 703057) accurately identifies the possibility of inadvertent engine cut due to similarity between the chop collar and the collective friction control on other aircraft. Three hazards which are written up together in this section of the report address two different problems: inadvertent operation and single point failure. Two of the hazards (Nos. 703054 and 703055) address two subtly different types of single point failures. Beginning with the January 1980 System Safety Statement,[c] the subtle distinction is dropped and the two hazards are replaced by one hazard (No. 70401) which addresses single point failure. This hazard is reported as being closed by virtue of the use of dual-redundant chop circuits and switches. While descriptions of the chop collar control appear in subsequent safety statements, the hazard of inadvertent actuation seems to have "fallen through the cracks," until it caused two Class A mishaps nine years later.

3.5.3 Systematic Hazard Closeout Process.

The Army has no systematic hazard closeout process.

A problem related to the lack of hazard tracking is the lack of a systemic hazard closeout process. There is no specific procedure or checklist to ensure that the identified hazard has been assessed, controlled with control measures verified, accepted by the contractor and the Army, and administrative control measures incorporated in manuals and training materials. Without a closed-loop hazard closeout process, system safety working groups and acquisition managers may overlook details in the acquisition process required for effective hazard control.

3.5.4 Hazard Information Provided to Acquisition Players

Relevant system safety information has not been provided to all players in the acquisition process to support effective accomplishment of their system safety responsibilities.

Hazards information is only communicated to the tester in terms of whether a system is safe to test and under what conditions. Information provided to testers has not included a listing of all identified hazards and control measures. Therefore, Test and Evaluation Masterplans (TEMPs) and Test Design Plans (TDPs) do not provide an adequate basis for safety testing. Certain hazards associated with performance requirements in the specifications or previously identified as deficiencies during testing received attention. However, many identified hazards were not communicated to the tester because control measures had been taken and no related mishaps had been recorded. Therefore, testing does not systematically evaluate the adequacy of control measures for all identified high-severity hazards (see 3.3.3).

Guidelines have recently been developed regarding the content of Safety Assessment Reports (SARs) prepared by contractors or materiel developers.[d] These guidelines require

"a comprehensive evaluation of the safety risks being assumed prior to test or operation of the system or at contract completion."

One purpose of the SAR is safety of testing, but it summarizes prior system safety data and may be used to communicate hazard information for safety verification purposes, as well.

Regardless of the mechanism, care must be taken to ensure that available hazard information is translated into the necessary critical issues in the Test and Evaluation Master Plan (TEMP) and the test design plan.

Decision makers above the PM receive only hazards information on selected hazards. The decision-making process tends to limit the hazard information that is provided to higher-level decision makers, who are primarily interested in issues that would prevent the system from moving into the next phase of development. Only recently has the USASC begun to provide an independent system safety assessment for MADP milestone reviews. This independent line of reporting helps ensure that all significant residual

---

(a) Jacobs, R.L., *System Hazard Analysis Report, Report No. 77-HA-8004, DAAJ01-77-C-0064*, Hughes Helicopters, June 1975.

(b) Jacobs, R.L., *System Safety Statement for the Phase 2 YAH-64 Advanced Attack Helicopter, Report No. 77-SS-0010, DAAJ01-77-C-0064*, Hughes Helicopters, December 1977.

(c) Johnson, H. and Morris, R., *System Safety Statement YAH-64 Advanced Attack Helicopter, Report No. 77-SS-0016, DAAJ01-77-C-0064*, Hughes Helicopters, January 1980.

(d) Mossa, M. et. al., *Guide for the Development of Safety Assessment Report (SAR)*, USACSTA-5472, U.S. Army Combat Systems Test Activity, Aberdeen Proving Ground, MD, August 1987.

hazards reach the decision makers and counters the "silent safety program" image that was noted in the NASA Challenger accident investigation.

Combat Developers have not received early information on hazards in order to provide input on the reasonableness and adequacy of control measures at a point when alternative control measures could be more readily implemented.

3.5.5 Communicating Risk to Decision Makers

Simple hazard descriptions and risk-assessment information alone are insufficient for making risk-management decisions.

The decision maker needs to have a sense of the projected "costs" of hazard acceptance. These costs include expected dollar losses from deaths, injuries, or occupational illness or damage or loss of equipment or property. Programmatic and mission impacts of hazards must also be considered as part of the "costs" in risk-management decisions.

Risk information provided to decision makers varied considerably. Safety Certificates of Materiel Release and Safety and Health Data Sheets sometimes included just a description of the hazard and how it was identified. Sometimes it included a Risk Assessment Code (RAC) including qualitative hazard severity and probability levels from MIL-STD-882.

Developer's safety reports and user and technical test reports provide the basis for risk assessments. For example, estimated failure rates were provided for components of the TOW missile in the failure mode and effects analysis for the launch and flight motors in the safety statement.[a] The TACOM safety office used test data to provide descriptions and assessment information on various HMMWV hazards.

Risk information provided to decision makers is not communicated in terms that can be easily compared in trade-off decisions. The HMMWV brake hazard descriptions did not include any projections of dollar losses, loss rates, or of the mission impacts the brake hazards might have in the field.[b] It also did not suggest programmatic impacts, such as costs for parking brake retrofits. Such information would have provided the decision maker with the "costs" of risk acceptance for comparison with system performance, schedule and cost.

Although the conflict between the BFV noise hazard and communication was described by the TACOM safety office,[c] no projections were made of potential hearing losses or mission impacts from this hazard. Interviews of 43 BFV crew members during this study revealed that only one person used double hearing protection. Most reported that it interfered with communication. The Army Environmental Hygiene Agency reported that limited audiometric data on armor senior sergeants (MOS 17Z) indicates that 41 of 177 (23 percent) individuals tested have suffered a compensable hearing loss. In 1987, Army compensation claims where hearing loss was the primary disability amounted to $177,316,500.[d]

For the HMMWV troop carrier, which has no rollcage or seatbelts for troops transported in the cargo area (see 3.1.5), no comparisons of costs to projected losses were found to support a decision by the Army to accept this risk.

3.5.6 Providing Safety Information to the Field

Field organizations have trouble keeping up with the current status of safety information.

Both the Ft. Lewis and Ft. Hood installation safety offices identified problems tracking safety messages, such as Safety-of-Use, Safety-of-Flight and Ammunition Suspension messages. These tend to be received from multiple sources and, in some cases, have not been sequentially numbered. There is no single source where an individual can go to ensure that one of these messages has not been missed or to determine the status of restrictions that may have been imposed.

One of the BFV trim vane collapse mishaps noted that the trainers were not aware of special strapping procedures recommended in a Safety-of-Use message to secure the locking link and release lever.

A BFV swim task force report[e] stated,

"The observation that the field does not have complete sets of technical manuals and change packages parallels an incompleteness in Safety-of-Use messages. Units do not reliably receive these water operation related messages....

(a) Dichter, H.S., *Engineering/Service Test Safety Statement Tow Heavy Assault Weapon, Report No. TOW-T20*, DA-01-021-AMC-13626(Z), Hughes Aircraft Company, Culver City, California, July 1966.

(b) Jarvis, G.G., Certificate of Materiel Release (HMMWV Utility Vehicles), TACOM, AMSTA-CZ, 19 June 1985.

(c) Certificate of Materiel Release (M2/IFV and M3/CFV with TMDE (STE-M1/FVS and DSESTS-M1/FVS), TACOM, AMSTA-CZ, 22 December 1982.

(d) Telephone conversation with the AEHA Hearing Conservation Office, Aberdeen MD regarding audiometric data maintained in the Ft. Detrick, MD data center, April 21, 1988.

(e) Singh, G.B., et. al., *PMO Sponsored BFV Swim Task Force, FMC Final Report*, STS VI, Contract DAAE07-86-C-R128, W/D 100-430-606, FMC Corporation, Ordnance Division Engineering, San Jose, CA, December 1986.

Field personnel apparently do not know what basic documents they should have, and do not know what revisions apply to those documents. This observation includes Safety-of-Use messages. The task force found no evidence of a 'closed loop' system."

The increase in the number of special safety messages to the field for the selected systems compared to prior systems is indicative of the complexity of newer systems. It is also reflects increasingly conservative public safety expectations that influence contractor and the Army safety management practices. However, the problem is not the reduction of safety messages; it is the reduction of the residual hazards which make such messages and restrictions necessary.

3.5.7 Feedback on Safety Performance of Systems

Contractors have had problems obtaining adequate feedback on the safety performance of their fielded systems.

In the past, contractors did not automatically received mishap and other safety performance data on their fielded systems. This impeded timely identification, evaluation and resolution of hazards. Contractors can now make a one time request to receive quarterly reports of mishap data for the duration of their contract. Most contractors depend on the Army for feedback on system safety performance.

Contractors for major systems may have representatives in the field as independent sources of hazard information. Such information can provide an independent check on the safety performance data collected in the ASMIS system. The contractor for the BFV tracked a list of current residual hazards obtained from field representatives and reported on the status of each open item at quarterly meetings with the PMO's system safety working group. Specific mishap data on turret door crushing mishaps was requested from the ASMIS data base by the contractor to confirm its reports.

Both Army and contractor system safety personnel reported that Army mishap reports for ground systems do not contain sufficient detail to serve as a good system safety tool. The DA 285 mishap report forms lack necessary system safety and human factors data to perform detailed causal analysis. Often the quality of the report is poor because the form is completed by a "unit safety officer" having little or no training in accident investigation and its relationship to system safety. Installation safety offices that provide training for the unit safety officers are frustrated by the high turnover rate among unit safety officers. There is no military occupational specialty (MOS) for these individuals similar to that for aviation safety officers, and mishap investigation is often viewed in terms of fault finding rather than mishap prevention.

For mishaps that require investigation by the installation safety office, notification often occurs days to weeks after the mishap has occurred, making it very difficult to conduct a worthwhile investigation. One of the TOW launch motor case rupture incidents involving National Guard exercises at the Yakima Firing Range was not reported to the Ft. Lewis safety office until over three weeks after the incident, when heavy damage to the launcher was noted by maintenance personnel.

System safety personnel indicated that mishap reports provide a sense of potential problems, but they rarely pinpoint a residual hazard because they lack the necessary specificity. For this reason, system safety personnel use various data sources to obtain further clues to residual risks. The use of EIRs and QDRs to supplement mishap reports was infrequent but useful when provided. Some significant TOW system safety incidents were identified through firing reports rather than in the mishap data base, because they did not meet reportability criteria: the missile was considered to be expended, so no loss was incurred.

3.6 Other Contributing Factors

Some causes of residual hazards were difficult to link to specific hazards, because they are even more fundamental in nature than most of the causes previously discussed and apply across the residual hazard source categories. They are derived from an overview of the reasons behind the prior systemic causes of residual hazards.

3.6.1 Perceptions of System Safety

System safety is not yet fully recognized as a legitimate discipline within the Army.

System safety is still viewed as common-sense prevention of accidents rather than a contributor to the operational effectiveness of systems. It is perceived as a safety office program rather than an acquisition program.

Evidence of this perception can be seen in the lack of system safety resources in key Army organizations. The two principal evaluators of major Army systems are the Army Materiel Systems Analysis Activity (AMSAA) and the Operational Test and Evaluation Agency (OTEA). Neither organization has system safety professionals even though safety is a critical factor affecting system performance and suitability. TRADOC which has the critical task of establishing safety performance requirements in requirements documents has just begun to hire entry level system safety personnel at a few of its centers and schools. OTEA

and TRADOC, the user test organizations, have traditionally assumed that TECOM performed all relevant safety testing and, therefore, no system safety expertise was necessary to support user testing.

PMs and PEOs have had little opportunity to learn about system safety other than through regulations and limited contact with safety engineers. Supporting safety offices reported that some development programs that had reported directly to AMC rather than the major subordinate command exhibited more independence and were less receptive of support from the MSC safety office. Concern was expressed that reorganization of program/project management with separate channels to DA might have a similar effect. Avoidance of the system safety program may be an indication of a lack of understanding about system safety.

3.6.2 System Safety Roles

Army system safety engineers view their role as program oversight rather program participation.

This has been a conscious choice, based on the perceived need to maintain independence from the PMOs in order to act as "honest brokers" regarding safety positions. Consequently, the system safety program is more reactive than proactive; more watching than doing; more an outside consultant than part of the acquisition team.

This lack of direct system safety involvement can result in delayed system safety decision making by the PM and the potential to leave supporting system safety personnel out of the hazard resolution process. If hazards must be resolved later in the development process when time and funding constraints are tighter, there is a greater chance that administrative controls rather than engineering controls will be used to correct hazards.

3.6.3 Motivating System Safety Excellence

There are insufficient incentives for contractors or acquisition managers to promote system safety excellence.

Lack of incentives tend to produce systems that only meet minimum safety requirements.

A specific issue mentioned by contractor system safety personnel was the problem of early involvement, especially when the program involves numerous subcontractors. Contractors must minimize their out-of-pocket costs of responding to Requests for Proposals (RFPs). However, it is usually necessary to develop preliminary design concepts for the response. If system safety personnel have not contributed to the design concepts at this initial stage, they may never be able to fully meet the system safety goal expressed in MIL-STD-882,

"...to make sure safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities, and their interfaces."

One contractor system safety manager indicated that his organization had adopted a policy to incorporate a minimum essential system safety program under its product assurance program, even where no system safety data items were required, simply because it made good business sense. This is a fairly recent change that was motivated not only by the payoffs of early system safety involvement, but also by liability considerations. He indicated that this was the result of extensive briefings to management. Prior to this policy, if there were no system safety data items, there was no system safety program. Another contractor safety engineer indicated that his organization only did what was required by contractual data items. He said that his management was responsible for returning a profit to the company, and no unnecessary funds were spent on system safety. These two views represent the two ends of the spectrum. Much of the difference lies in how management perceives the system safety program. There appears to be a trend toward the more enlightened view, as contractor managers gain an understanding of the system safety function and how it contributes to bottom-line profits.

The responsibility for evaluation of PM and PEO system safety programs has shifted to the USASC since the reorganization. The AMC Field Safety Activity, which had this responsibility prior to reorganization, could find only one system safety evaluation that had been conducted for any of the PMOs of the systems selected for this study. This 1984 evaluation[a] was requested and funded by the PM for the BFV. It commended the PM for formally establishing a Safety Review Board in 1982 to coordinate dissemination of system safety information to the field, but recommended improvements to obtain better feedback from the field.

(a) Cates, C.A., Chew, D.A., and Medina, L.J., *System Safety Field Audit of the Bradley Fighting Vehicle Systems*, U.S. Army DARCOM Field Safety Activity, Charlestown, IN, January 1984.

3.6.4 System Safety Planning

Acquisition managers have not had a sound basis for developing an adequate system safety program and determining the necessary level of system safety resources.

Neither Army nor contractor system safety support requirements for new system acquisition have been based on documented risk or loss projections for the system. Supporting safety offices have considered system safety as the PM's responsibility, while PMs have considered it to be the responsibility of the safety office. Therefore, support has been based on the availability of system safety engineers in the supporting safety office. The Apache was one of the first Army aircraft to have a contractual requirement for a system safety program. The Army Aviation Systems Command (AVSCOM) had only two system safety engineers to provide all Army aviation system safety support during the early stages of the Apache program, when it was most critical. Recent requirements for PMs to develop System Safety Management Plans may help to drive development of methodologies for predicting life-cycle mishap losses as a basis for system safety planning.

Part of the reason for the limited involvement of Army system safety engineers is that each engineer may provide system safety support for as many as 20 to 30 systems, with most being fielded systems. There are simply too few system safety engineers to actively cover changing workload demands of the PMOs.

Effective system safety programs require qualified system safety support. The number of special safety messages and restrictions following fielding of emerging systems is an indication of the need for the PM to have system safety expertise available to hit the road running on a new program.

Since sufficient system safety resources have not been available from the AMC MSCs to meet the work demands, the PMOs have assigned system safety duties to non-system safety professionals on their staffs. This has resulted in system safety tasks being divided between individuals with limited expertise and high involvement and system safety engineers with high expertise and limited involvement. This is a suboptimal allocation of resources.

There has not been a well-balanced investment of system safety resources within the Army compared to the system safety role of each Major Army Command (MACOM). AMC took an early lead in system safety and developed an in-house system safety engineering intern program to provide its own qualified system safety support. The other MACOMs have only recently begun to assume their roles within the Army system safety program.

3.6.5 Documentation for Developing Lessons Learned

Documentation of hazard identification, assessment, control and risk management is not maintained and compared with fielded system performance to develop future system safety design and management lessons learned.

One of the problems of developing system safety management lessons learned for this study has been the difficulty of obtaining the necessary documentation to track residual hazards through the acquisition process. While the PMO has usually had the most complete acquisition record, this documentation has often been scattered among various staff members. The acquisition history is gradually lost due to space limitations, paper reduction programs, and older documents being replaced as the development process progresses. There is no "system library" of reports and significant correspondence kept for development of lessons learned. Some reports were available through the Defense Technical Information Center (DTIC), but these were also limited.

3.6.6 Risk Acceptance

Perceived risk appears to influence risk management recommendations and decisions.

Army risk acceptance appears to be tied to the level of user control over the hazard. In a missile system like the TOW, the threshold for risk acceptability appears to be lower than in a vehicle like the HMMWV or the BFV.

Perceived risk may also contribute to a resistance to change design configurations for hazards which have been historically accepted. The association of the jeep with rollover mishaps has been accepted for generations of jeeps prior to the HMMWV. The lack of rollover protection and seatbelts in the cargo area of the HMMWV troop carrier may be another example of resistance to change (see 3.1.5).

The impact of perceived risk on Army risk management decisions has not been examined but is likely to have other ramifications for acquisition managers. The body of research on perceived risk may well have other implications for decision makers. It might be predictive of conflicts between the Army and congress or the public regarding acceptability of risks.

4.0 System Safety Management Lessons Learned and Recommendations

System safety management lessons learned were aggregated from related systemic causes of unexpected residual hazards in fielded systems. Such hazards were unexpected in that they were either never identified or the severity or frequency of resulting mishaps was not anticipated. This section presents the lessons learned and the resulting recommendations. Additional areas of research suggested by this study are listed in Appendix B.

4.1 A Proactive System Safety Program

The role of Army system safety professionals must strike a balance between oversight and increased direct involvement in system acquisition to make the best use of limited system safety resources.

System safety is a knowledge-based discipline. Its specialists must be located where they will have maximum impact on total system design, both in terms of types of inputs and timeliness of inputs in the acquisition process. The best use of the Army's qualified system safety engineers is in the game, not watching it. Drucker (1988) notes that the optimum organization for a knowledge-based discipline has a limited investment in the management structure in order to maximize utilization of technical expertise at the operational level.

Army system safety engineers should be involved in development of safety performance requirements in requirements documents, system safety working groups, resolving system safety issues with contractors on behalf of the PM, technical design reviews, test planning and participation in specific safety tests and fielded system reviews. Peer review, independent reporting channels, and independent evaluation will be required to maintain independence. Peer review can be provided by supporting safety managers who review all work of their system safety engineers. The USASC is now providing an independent safety assessment to MADP reviews for major systems. AMC's MSCs have an independent reporting channel to AMC for other systems. AMC's Field Safety Activity and the USASC can ensure that independence is maintained through their evaluations.

Recommendations:

USASC/AMC

Develop the necessary policy to provide a more proactive role early in the system acquisition process for Army system safety engineers supporting PMOs.

4.2 System Safety Training of Acquisition Players

System safety training should be provided for all supporting acquisition players to provide a proper understanding of their system safety roles and objectives.

This is essential for acquisition managers who have the primary responsibility for the safety of the systems being developed. System safety training should be integrated into existing courses, or special courses should be provided.

Including system safety as one of six domains under the MANPRINT program has left Army system safety personnel with concerns about resources, program visibility, potential to dilute safety issues, etc. This apprehension has been increased by the relatively low emphasis on system safety in MANPRINT training programs.

Recommendations:

AMC/TRADOC/OTEA

Provide system safety training for all technical and user testers. Review system safety training materials presently used in training test engineers at the Combat Systems Test Activity for possible use. Provide sufficient qualified system safety personnel to support test directors in the planning and conduct of testing.

USASC

Ensure that the USASC system safety course for PMOs is integrated into required courses for future PMs. Recommend that a video system safety course be made available to other acquisition players with tailored handout materials; e.g., tailored for Human Factors Engineers.

Review and provide system safety input for MANPRINT training courses.

4.3 Planning for System Safety

Plans for implementing a system safety program within PMOs should be based on projected life-cycle losses of the systems being acquired.

PMs and PEOs must have a supportable plan for accomplishing necessary system safety tasks. The System Safety Management Plan (SSMP) has been established for this purpose. This plan must provide a rationale for tailoring the system safety process that will stand up to critical review. This requires that the extent of the SMMP be based on the projected level of risk for the system being developed.

Recommendations:

USASC
Develop a methodology for estimating life-cycle losses that can be used in development of System Safety Management Plans for PMOs and include this information in DA Pam 70-2 and DA Pam 385-16.

4.4 System Safety Resources

Requirements for system safety resources and the means of providing those resources should be established at the outset of the acquisition program. To provide the necessary resources for PMOs, contracts should be considered to supplement existing system safety support. Allocation of Army system safety resources should be based on commodity risks.

Currently, the level of matrixed support from the supporting safety offices is inadequate to accomplish required system safety requirements. Over a period of time, system safety management plans for PMOs may provide justification for increased system safety support from AMC MSC safety offices. However, to meet current needs, alternative means of providing adequate support are possible. The Blackhawk PM has recently obtained contract support of his system safety work, while the TACOM and MICOM safety offices report that they are considering the possibility of providing additional system safety support through technical support contracts.

The PMOs through collateral duty assignments are already funding a supplemental level of system safety support. While a single PMO may not be able to provide steady work for a full-time system safety staff member, system safety support requirements accumulated at the PEO level might.

System safety resources should be invested strategically according to projected loss rates and mission impacts of mishaps to maximize the influence of system safety on the design of emerging systems. This is true for both Army and contractor system safety resources.

The system safety program of one contractor has been organized in several ways over a number of years. It was concluded that placing the system safety engineers directly in with the design groups was the most efficient method for accomplishing system safety goals. Similar experimentation by PMs and safety managers could help to determine the optimum arrangement for achieving their mutual objectives.

Recommendations:

USASC
Through the System Safety Coordinating Panel, develop a long-term strategy for balancing system safety resources to maximize the effectiveness of the Army system safety program.

PMs/PEOs
Ensure that necessary system safety support for PMOs is provided, either from the supporting safety office or by contract.

4.5 System Safety Design Guidance

Designers must be aware of historic and state-of-the-art system safety design guidance to improve the safety of new generations of Army materiel.

Designers must know what worked in eliminating or controlling the hazards of related systems (Army and commercial); what went wrong and how to fix it (if feasible control measures are known); and what hazards are associated with new materials and technologies that may be adopted in new system development. To support designers, it is necessary to systematically capture system safety design lessons learned and keep them current with changes in technology.

Like any learning process, the gathering of hazard information and safety design lessons learned must be continuous. Lessons must reflect not only the means of dealing with past failures, but also successful design measures that have eliminated or controlled hazards effectively. Such safety design lessons may come from many sources: military and contractor research, development, test and evaluation; user feedback on systems; general industry; various safety organizations; and academia.

LABCOM and other organizations responsible for technology-base activities must actively seek and record hazard information associated with new technologies and materials that may be used in the development of future systems.

The MANPRINT data base being developed by MRSA may eventually provide a source of lessons learned for future systems. For each system, the system safety module will include a listing of residual hazards by subsystem. This data base has been designed, and MRSA is now in the initial data collection phase.

Recommendations:

AMC

Expedite the development of commodity-specific system safety engineering design guides and ensure that they are suitable for reference in requirements documents. Proponents for safety design guidance documents must update them as necessary to reflect changes due to improvements in technology.

Review the MANPRINT data base to ensure that it can be used efficiently to identify, develop and record safety design lessons learned. Care should also be taken to ensure database compatibility with inputs from appropriate MIL-STD-882 system safety data items to minimize input labor.

USASC/AMC/TRADOC

Recommend that system safety personnel in USASC and AMC's MSCs work closely with the new system safety staff members in the respective TRADOC centers and schools to ensure that requirements documents include adequate system safety performance provisions that incorporate safety design lessons learned.

USASC

Establish a focal point within the Army for coordinating safety design lessons learned. Ensure that commodity-specific safety design guidance is kept current and that lessons learned are gathered from all relevant sources.

Safety design lessons learned are only as good as the feedback provided. Review the mishap reporting format to ensure that it captures information essential for developing lessons learned, e.g., material failure and human performance information.

4.6 Consideration of Human Performance in System Safety

Since human error is a contributing cause in a majority of Army mishaps, human performance limitations must receive greater consideration during the selection and evaluation of control measures for severe hazards. Human factors engineers should review user-dependent hazard control measures to ensure that they are reasonable and effective.

The need for better integration of system safety and human factors has been a continuing issue at various safety forums within DoD and can be seen in the nature of the residual hazards noted in this study. Elimination of such hazardous situations in system design should reduce the potential for operator errors and permit users to concentrate more fully on mission performance.

All four of the selected systems were developed prior to the initiation of the MANPRINT program. Subsequently, there has been work to implement certain MANPRINT program requirements in the PMOs. System safety has a great deal of overlap with human factors engineering, health hazards assessment, and training. MANPRINT may well provide the opportunity for better lateral communication and integration of efforts among these disciplines if qualified system safety personnel participate in MANPRINT working groups.

Recommendations:

AMC/HEL/PM/PEO

Ensure that all catastrophic and critical hazards that rely on administrative control measures are reviewed jointly by system safety and human factors engineers. System safety engineers should determine that the system design conforms to the rules of system safety precedence. As a design goal, administrative control measures should be permitted only if engineering control measures are determined to be technically infeasible or not cost effective. Human factors engineers should assist in task analyses and predicting human error rates to support determination of whether user-dependent hazard control measures are reasonable and effective.

4.7 User Inputs to System Safety

The Army must promote greater customer participation in the system safety program to ensure realistic control of hazards in the use environment and enhanced mission performance.

Contractor and Army system safety personnel must have direct contact with users to understand aspects of the operational environment that may create or contribute to system hazards. They must also ensure that proposed control measures enhance rather than inhibit overall mission performance. This requires direct, frequent input from users throughout system acquisition. The Packard Commission recommended that PMs and PEOs have continuous communication with users. This recommendation must be applied to system safety personnel, as well; so that

the broader objective of system safety found in AR 385-16 can be met:

"maximizing operational readiness and mission protection through accident prevention by ensuring that appropriate hazard control measures are designed into the system."

Involvement of system safety personnel in observation of user testing or participation in fielded system reviews of the systems they support could help to identify hazards while at the same time providing direct contact with users.

Recommendations:

TRADOC
Ensure that input to requirements documents considers the impact of user practices and doctrine on system safety. Provide a mechanism to ensure that safety performance requirements are addressed in sufficient detail in requirements documents.

TRADOC/PM
Ensure that the system safety working group has user representation and that the contractor has access to users for design consultation purposes.

TRADOC/OTEA
Ensure that user testing determines not only if user-dependent hazard control measures can be accomplished but also whether they are realistic in an operational environment.

AMC
Require system safety participation in fielded system reviews to promote a better understanding of system use in the field and to obtain user feedback on residual hazards.

USASC
Consider the use of no-fault safety hotline numbers in user system manuals to facilitate hazard reporting.

Investigate methods for improving user system safety feedback through Logistics Assistance Offices.

4.8 Hazard Probability

Hazard probability must be expressed as a quantitative rate and interpreted in light of exposure in order to be useful in projecting losses for risk management decisions. Provide a standard method of predicting human reliability to reduce errors in assessing hazard probabilities involving human performance.

Without an adequate expression of hazard probability, risk management decisions must be made on "gut feelings." Hazard probability must include accurate estimations of the potential for human error and consider the expected exposure in the use environment.

Recommendations:

AMC/PMOs
Ensure consideration of exposure in the risk assessment process.

Hazard probability definitions should be tailored for the system. However, they should include incidence rates that remain constant regardless of the number of systems fielded or the life of the system. Hazard probability should be described as a rate that expresses the probability that a hazard will be created in so many operating hours, miles driven, operating cycles or other measure of use. This would facilitate loss projections and convey a more concise view of hazard probability.

USASC
Elevate MIL-STD-882B issues regarding hazard probability and exposure for consideration by the Joint Services Safety Conference's System Safety Seminar.

HEL/USASC
Develop a simplified standard method of providing order-of-magnitude predictions of human reliability (error rates) for hazards where user-dependent control measures are proposed.

4.9 Validation of Hazard Control Measures

Control measures for severe hazards must be systematically verified during testing.

At a minimum, the effectiveness of control measures for all high consequence hazards should be verified during testing. This requires that testers receive the necessary hazard information and that critical issues regarding validation of controls for specific hazards are identified in the Test and Evaluation Master Plan and the Test Design Plan.

Recommendations:

AMC/TRADOC/OTEA
Ensure that all prior hazard information is used in the planning of tests. Testing should verify the resolution of all severe hazards, including user-dependent control measures, regardless of compliance with standards.

4.10 Communicating Risk to Decision Makers

Safety risks should be communicated to decision makers in terms of projected loss rates and programmatic and mission impacts that may be expected if a hazard is accepted.

Decision makers need to know what they can expect when they accept a hazard. All severe hazards must be characterized not only in terms of hazard severity and probability, but also, to the extent possible,in terms of loss rates and programmatic and mission impacts of associated mishaps. Without such projections, it is often impossible to later say whether systems are performing up to the Army's expectations when actual fielded system safety performance is assessed. For this reason, it is good to estimate loss rates and associated uncertainties.

Recommendations:

AMC/PMs/PEOs

Ensure that hazard information going to decision makers includes projected loss rates, and programmatic and mission impacts of mishaps.

4.11 Risk Management

Risk management decisions must be made at a management level commensurate with risk and documented.

Hazard severity tends to be accurately assessed early in system development. Hazard probability assessments are much more tentative in the early stages. The PM and system safety working group need to begin acting as soon as severe hazards are identified. Risk management must be a continuous process.

Risk management decisions must be documented to ensure that acceptance of hazards involves conscious management decisions.

Recommendations:

AAE/PEO/PMs

Ensure that risk management is a continual process in order to resolve system safety issues as early in the development process as possible.

All identified hazards must be considered in the risk-management process and decisions documented in a hazard tracking system. This process should reflect Army management's position on the adequacy of hazard control measures taken by the contractor. Administrative control measures should be accepted only where engineering controls are not technically feasible or cost effective. However, this design objective may not be met due to the exigencies of funding and schedule constraints. In such cases, it is critical that decisions are documented. The AMC MSC safety office supports this process, but the final responsibility rests with program management.

Risk-management decisions should be made by a level of management commensurate with the level of risk.

4.12 Communicating Hazard Information

All players in the acquisition process must have access to relevant hazard information to do their jobs properly. Significant system safety documentation must be maintained for comparison of risk management expectations with the safety performance of the fielded systems and development of lessons learned.

Hazard communication is the glue than binds the other elements of the system safety program into an effective barrier against unexpected residual hazards in fielded systems. Safety-relevant documentation must be maintained if the system safety and risk management programs are to be improved through the development of lessons learned.

A hazard tracking system should be a continuous thread that runs throughout the acquisition process. It should capture all hazards identified in contractor analyses and testing, help to identify issues that require cooperation between system safety and interfacing disciplines, provide the basis for planning safety testing to determine the adequacy of control measures for severe hazards, support a determination of the conditions under which the item is safe to test, and provide a tool for ensuring that the contractor and Army system safety and management agree that the proposed method of control is adequate. A hazard tracking system should be the basis for risk management decisions throughout the acquisition process, because such a system presents a snapshot of the system's safety status and provides a convenient place to document prior risk management decisions. A hazard tracking system should also be used as a checklist for evaluating safety guidance in manuals and training programs. Finally, it can serve as the baseline for tracking the safety performance of newly fielded systems and for performing fielded system reviews.

Recommendations:

AAE

Require that the PM or managing activity use a hazard tracking system and maintain significant acquisition

documentation throughout the acquisition process to support development of system safety management and technical lessons learned.

Upon deprojectization of the PMO, acquisition documents should be maintained by the item manager or be maintained by system at the MSC's technical library or other location where they would be readily available for review. Consideration should be given to use of electronic storage mediums to reduce space and permit computerized search capabilities. The hazard tracking database should be maintained by the supporting safety office following deprojectization.

USASC

Establish requirements to support hazard tracking throughout the system life cycle as the basis for hazard communication. Hazards must be uniquely identified and should not be dropped even though they are considered to be "closed out." This database should contain the history and current status of each hazard associated with the system.

Recommend that either the ASMIS system or a database accessible via the safety electronic mail system be used to provide a single source of information on the status of safety messages to the field.

4.13 Hazard Closeout

There must be a systematic hazard closeout process to ensure that necessary steps for hazard resolution are not overlooked.

A systematic hazard closeout process is not possible without an adequate hazard tracking system. A closeout process provides acquisition management with a scoreboard for hazard resolution.

Recommendations:

USASC/AMC/PMs/PEOs

Provide policy and procedures to ensure that a systematic, closed-loop process exists for closing out hazards and that safety analyses are reviewed and updated as system modifications are made.

4.14 System Safety Incentives

The system safety performance of acquisition managers and contractors must be routinely evaluated. Investigate the feasibility of using performance award contracts to reward system safety excellence.

Aside from contractual requirements, the contractor's system safety program is motivated by liability, cost and image considerations. The key to immunity under the "military contractor's defense" is that the contractor provided a system according to government specifications and that the contractor fully disclosed the hazards associated with that design. Typically the contractor has the responsibility to correct all deficiencies up to the point of type classification. Thus, system safety efforts can save the contractor money that would be spent on safety-related retrofits. Finally, future government contracts depend on the contractor's reputation, which depends largely on past product performance. Having a product that is widely considered to be hazardous can be a serious deterrent to future business. These factors are changing contractor management views of the system safety function.

In July 1986, the Assistant Secretary of the Army for Research, Development and Acquisition announced that MANPRINT would be a separate area of consideration in awarding contracts. This could help to provide the necessary incentive to ensure early involvement of system safety in the design effort if such expectations are expressed in RFPs.

Recommendations:

AAE

Investigate the feasibility of using performance award contracts to reward system safety excellence by contractors. Beyer (1987) provides a guide for use of award fee contracts and their application to system safety. If feasible, such contractual means should be implemented on a trial basis to determine their potential to motivate contractors to integrate system safety and design efforts from the inception of the development effort.

USASC/AMC

Develop objective, efficient measures of system safety performance for the acquisition process. Two ideas worthy of study are comparison of actual cost data to projected safety-related retrofit costs and to fielded loss rates.

As a minimum, compare PM and PEO system safety performance with Army expectations expressed in their charter and in AR 385-16. Actual bottom line safety performance of the systems they manage could also be used when measures of performance are developed. The performance of all organizations with system safety functions should be periodically evaluated during MACOM reviews by USASC and by MACOM safety reviews of their subordinate commands.

5.0 Army Review of the Study

The Technical and Executive Subpanels of the Department of the Army System Safety Coordinating Panel have reviewed this study. Their comments have been considered in completing this final technical report. This section summarizes the broad areas addressed in these comments.

Opinions have been divided regarding the role of Army system safety personnel. There was concern that system safety members of the PM's team cannot provide independent oversight of their own work. There was also concern that Army system safety personnel need to be actively involved in the acquisition of new systems as early in the process as possible. We have tried to find a means of satisfying both objectives rather that viewing this as an "either or" situation.

There have been some comments that would suggest that most of the lessons learned have now been addressed by MANPRINT. The sense of this study was that the MANPRINT program has the potential to address specific lessons learned. However, the program in practice has not yet resolved the problems noted. This is a relatively new program, and it would take a separate evaluation to determine the extent to which the MANPRINT program has addressed the systemic causes of mishaps noted in this study.

A final concern has been that acquisition managers must maintain their perogatives in making tradeoff decisions. Acceptable risk decisions are always a value judgement. It is the responsibility of system safety personnel to effectively communicate risk information to Army managers in support of the risk management process.

Certain Army organizations have already taken steps to implement applicable recommendations of this study. This positive response is the best indication of the value of the methodology and results of this study.

6.0 Policy and Guidance Status Matrix

System safety management lessons learned were compared to current policy documents to determine the degree to which the deficiencies have been addressed. MIL-STD-882, DA Pam 385-16 and AMC/TRADOC Pam 70-2 (currently being revised as DA PAM 70-2) were included, because they are the primary guidance documents for contractors, system safety engineers, and acquisition managers, respectively.

Development of the four systems involved in this study took place over a 20-year period. During this period many organization and programmatic changes have taken place. The Army system safety program was in its infancy in the 60s. Many of the problems that were noted in the acquisition of these systems have been addressed as the Army system safety program developed. The matrix in Figure 7 provides a measure of the progress that has occurred in the system safety program. This matrix also indicates areas where policy needs to be improved. Specific recommendations for improvement of policy are provided in Appendix B.

This study has noted systemic causes of residual hazards. These causes are an indicator of problems in either policy or its implementation. The matrix below indicates the existence of policy; it does not indicate the effectiveness or the degree to which current policies are being implemented. Army acquisition and system safety management must take the lead in routinely evaluating these factors.

POLICY/GUIDANCE DOCUMENTS

A. MIL-STD-882B
B. AR 385-16
C. DA Pam 385-16
D. AR 70-1
E. AMC/TRADOC Pam 70-2
F. AR 70-10
G. AR-70-17
H. AR 71-3
I. AR 602-2
J. AR 700-142

System Safety Management Lessons Learned	A	B	C	D	E	F	G	H	I	J
1. A Proactive System Safety Program		◗	●	○	●	○	◗		●	
2. System Safety Training		◗	●			○		○		
3. Planning for System Safety	●	◗	●	●	◗		◗	◗	●	
4. System Safety Resources		○	○	◗	◗		◗	○	●	
5. System Safety Design Guidance	●	◗	◗	○	◗				◗	
6. Consideration of Human Performance	●	◗	◗	○		◗			◗	
7. User Inputs to System Safety	○	●	◗	○	◗	◗	◗	◗	◗	○
8. Hazard Probability	◗	●	◗							
9. Validation of Control Measures	○	◗	◗		○	◗	◗	○	◗	○
10. Communicating Risk to Managers		●	●			◗		●		
11. Risk Management	●	●	●	◗	◗		◗		○	◗
12. Hazard Closeout	●	○	○	○			○		●	◗
13. Communicating Hazard Identification	●	◗	◗	◗	◗	◗	◗	◗	◗	◗
14. System Safety Incentives		●	●	○					●	

KEY: No symbol indicates that the lesson learned is not relevant for the given policy document.
○: The lesson learned is not addressed
◗: The lesson learned is partially addressed
●: The lesson learned is adequately addressed

Figure 7. Matrix of Lessons Learned vs. Army Policy

7.0 Conclusions

This study has confirmed that many contributing causes of mishaps can be traced back to the acquisition process and the system safety program, which is an integral part of that process. Dr. Sculley, ASA(RDA) has appointed the PEOs to be System Safety Officers for their systems.[a] PMs are charged with responsibility for the safety of their system by regulation and charter. With support from all players in the acquisition process, the PMs and PEOs are in a position to control the level of safety risk accepted by the Army. Continuation of strong leadership and direction will be necessary to ensure that these initial efforts show results in terms of reduced residual hazards in emerging systems.

Much progress has been made in the system safety program since its inception, as reflected in the degree to which current policy documents address the lessons learned. Existence of policy is no guarantee that the necessary practices are being implemented. This highlights the need for periodic evaluations of PMOs to determine the degree to which these policies are being implemented.

Improvements in the safety of fielded systems will require not only changes in practices but also in attitudes concerning system safety and perceptions of the role of Army safety engineers in the acquisition process.

Improvements will require active involvement of safety engineers in the PM's system safety working group to resolve hazards in a timely manner. PMs and PEOs will have to build effective acquisition teams that include system safety engineers.

A long-term strategy is necessary to bring about these changes and implement the system safety management lessons learned. This may require development of new methods for evaluating the effectiveness of the risk management process to determine the optimum levels of system safety support for acquisitions of various classes of systems. The systems selected for this study have shown several system safety successes that demonstrate its value. Preventing just one Apache loss could fund all Army system safety engineers for over two years.

The recommendations derived from the system safety management lessons learned provide guidance for addressing the major systemic causes of unexpected residual hazards in fielded systems.

These recommendations support the acquisition manager because they 1) help deliver a safer, more effective system 2) reduce retrofit and life-cycle system costs 3) reduce acquisition program delays and restrictions. The system safety program achieve these benefits by ensuring early hazard identification, correct hazard assessment, effective hazard control, improved risk management, and improved communication of relevant hazard information. The specific policy changes necessary to effect these recommendations are provided in Appendix A.

Acquisition managers are concerned with management risk-taking in the decisions that they must face. MacCrimmon and Wehrung (1986) identify three risk factors related to management risk taking: lack of control, lack of information, and lack of time. The system safety management lessons learned identified in this report can aid the acquisition manager by reducing the management risk involved in safety risk acceptance.

(a) Letter on System Safety, ASA(RDA), 18 August 1987.

References

1. Bell, B.J. and Swain, A.D., Overview of a Proceedure for Human Reliability Analysis, Hazard Prevention, January-February 1985.

2. Beyer, J.N., "Award Fee Guide for System Safety Professionals", Proceedings of the Eighth International System Safety Conference, New Orleans, System Safety Society, Sterling, VA, July 27-31, 1987.

3. Drucker, P.F., "The Coming of the New Organization", Harvard Business Review, January-February 1988.

4. Johnson, W.G., MORT The Management Oversight and Risk Tree, SAN 821-2, UC-41, U.S. Atomic Energy Commission, February 1973.

5. Logan, H. L., The Stress Corrosion of Metals, John Wiley & Sons, New York City, NY, 1967.

6. MacCrimmon, K.R. and Wehrung, D.A., Taking Risks, The Management of Uncertainty, The Free Press, New York, NY, 1986.

7. Society of Automotive Engineers (SAE) 1984 Handbook, Volume 4: J374 Roof Crush Test Procedure, Society of Automotive Engineers, 1984.

8. Sweginnis, R.W., "System Safety and the RFP-The A to Zs", Hazard Prevention, July-August 1987.

9. U.S. Army Safety Center, "Human Error." U.S. Army Aviation Digest, March 1988.

Regulations, Manuals and Standards

10. DODI 5000.36, System Safety Engineering and Management, April 1986.

11. MIL-HDBK-759, Military Standardization Handbook Human Factors Engineering Design for Army Materiel, March 1975.

12. MIL-STD-882B, Military Standard System Safety Program Requirements, March 1984.

13. MIL-STD-1180B, Military Standard Safety Standards for Military Ground Vehicles, September 1986.

14. MIL-STD-1290(AV), Military Standard Light Fixed- and Rotary-wing Aircraft Crashworthiness, January 1974, with Notice 1, July 1977.

15. MIL-STD-1472C, Military Standard Human Engineering Design Criteria for Military Systems, Equipment and Facilities, May 1981, with Notice 3, March 1987.

16. AR 70-1, System Acquisition Policy and Procedures, 1988.

17. AR 70-10, Test and Evaluation During Development and Acquisition of Materiel, August 1975.

18. AR 70-17, System/Program/Project/Product Management, August 1985.

19. AR 71-3, User Testing, January 1986.

20. AR 310-25, Dictionary of U.S. Army Terms (Short Title: AD), October 1983.

21. AR 385-16, System Safety Engineering and Management, September 1985.

22. AR 385-40, Accident Reporting and Records, April 1987.

23. AR 602-1, Human Factors Engineering Program, February 1983.

24. AR 602-2, Manpower and Personnel Integration (MANPRINT) in Materiel Acquisition Process, April 1987.

25. AR 700-142, Materiel Release, Fielding, and Transfer, April 1988.

26. AMC/TRADOC Pam 70-2, Materiel Acquistion Handbook, March 1987.

27. DA Pam 385-16, System Safety Management Guide, September 1987.

28. TM 9-2320-280-10, Operator's Manual, (HMMWV), October 1986.

29. TM 9-2350-252-10-2, Operator's Manual Fighting Vehicle Infantry (M2/M2A1) and Fighting Vehicle Calvary (M3/M3A1) Turret, September 1986.

Appendix A

Recommended Changes to Army Policy and Guidance Documents

Appendix A

Recommended Changes to Army Policy and Guidance Documents

This appendix contains specific recommendations for changes to the principle Army policy and guidance documents associated with the Army acquisition process and system safety.

MIL-STD-882B

4.2 System Safety Program Objectives

Page 4. Change to read:
b. ... Risk shall be described in risk-assessment terms (see paragraph 4.5 below) with projections of loss rates and mission impacts.

Page 5. Add:
j. Human performance limitations are considered where administrative control measures are necessary.

Page 5. Add:
k. There is a continual risk management process to resolve system safety issues as early in the development process as possible.

4.3 System Safety Design Requirements

Page 5. Change to read:
... design of the system. When possible, user representatives should be consulted on the impact of the operational environment on safety requirements and hazard control measures. Some general system safety...

4.5.2 Hazard Probability

Page 7. Add:
Specific Individual Item***
***Assumptions regarding item utilization and life expectancy must be defined.

Page 7. Add:
An example of a quantitative hazard probability ranking is:

Description	Level	Hazard Probability*
FREQUENT	A	P > 10-2
PROBABLE	B	10-2 > P > 10-3
OCCASIONAL	C	10-3 > P > 10-4
REMOTE	D	10-4 > P > 10-6
IMPROBABLE	E	P < 10-6

* In 1000 hours or 10,000 miles of operation, or 1000 items expended for single-use items or other defined measures of exposure.

Page 7. Add:
4.5.3 Consideration of Human Performance. Care must be taken not to overestimate human reliability. It is necessary to consider exposure in addition to hazard probability when evaluating the adequacy of proposed user-dependent control measures.

Appendix A: Guidance for Implementation of System Safety Program Requirements

Page A-5. Add:
30.3.3 When considering user exposure or time-dependent events, it is necessary to consider the exposure in addition to normal hazard assessment parameters of hazard severity and probability. This is standard practice in consideration of health hazards and is useful when considering the simultaneous occurrence of events. Low hazard probabilities may be misleading as indicators of the need for corrective action if the frequency of exposure is high.

AR 70-1

2-1 Army Acquisition Executive (AAE)

Page 2-1. Add:
f. Serves as principal system safety manager for Army system acquisition and ensures that the levels of authority for risk-management decision making are commensurate with the the potential for loss and mission impact.

g. Ensures that all Army acquisitions use a hazard tracking system with a systematic hazard closeout process to ensure that acquisition managers have adequate information to support safety risk management decisions.

2-2 g. Specific PEO responsibilities include:

Page 2-2. Add:
(7) Serving as system safety officer for assigned programs and ensuring resolution of identified hazards to minimize future safety retrofit actions and mishap potential of fielded systems.

2-3 Project/Product Manager (PM)

Page 2-3. Add:
e. Develops and implements a system safety management plan in coordination with the system safety working group to ensure that system hazards are identified, risk is assessed, and hazards eliminated or controlled and the adequacy of control measures verified. System Safety resource requirements should be based on the projected life-cycle loss potential of the system. Ensures that residual hazards are elevated to the appropriate decision authority and risk management decisions documented. (See AR 385-16.)

2-X Chief of Staff, Army (CSA)

Page 2-3. Add:
The CSA, through the Director of Army Safety (DASAF), will establish system safety policy for system acquisition and evaluate system safety performance.

2-19 CG, TRADOC

Page 2-11. Add:
c. (x) Provide user consultation to system safety working groups and contractor design and system safety personnel.

AR 70-10

2-6. User testing

Page 2-7. Add:
a.(5) whether user-dependent hazard control measures are effective and realistic in a tactical environment.

2-21. Safety testing.

Page 2-12. Change to read:
... throughout all TT and UT. System safety training will be provided to all test directors. Sufficient qualified system safety engineers are required to support test directors in the planning and conduct of specific safety tests.

Page 2-13. Add:
b.(7) Test planning will use all prior hazard information contained in the hazard tracking file. As a minimum, testing will verify the adequate resolution of all severe (catastrophic and critical) hazards, including user-dependent control measures. Technical testing will verify the adequacy of engineering and administrative control measures. User testing will verify the adequacy of user-dependent control measures in the use environment.

AR 70-17

2-3 Role and authority of the PM

Page 6. Change to read:
(16) Insure that adequate resources based on life-cycle system loss projections are provided to minimize mishap potential in the fielded system. Organize a system safety working group with user input to support the program manager in developing and implementing his System Safety Management Plan (AR 385-16). Insure that hazards are tracked and that there is a systematic hazard closeout process....developmental

and operational testing. The adequacy of control measures for all identified severe hazards must be verified during testing.

AR 71-3

5. Policy

Page 3. Change to read:
5k ...after a safety release with supporting safety and health data, e.g., Safety Assessment Report (SAR) and Health Hazard Assessment Report (HHAR), has been provided and is accepted by the tester (AR 385-16). Testing will validate user-dependent hazard control measures for all severe hazards (Hazards with critical or catastrophic severity levels when risk is assessed IAW AR 385-16) identified in test issues and criteria, the SAR and the HHAR and ensure that they are realistic in the use environment. The UT...

6b(3) CG, OTEA

Page 4. Add:
Ensure that necessary specialized training is provided for user test directors, including system safety and test incident investigation.

Page 4. Add:
Provide resources to proponent centers and schools to perform system safety tasks within TRADOC, including support of user testing.

7. Functional user test participants

Page 5. Add:
a.(1) Provide system safety engineers to monitor user testing when necessary to resolve safety issues.

Page 5. Change to read:
a.(2) ...and safety release with supporting safety and health data, e.g., Safety Assessment Report (SAR), Health Hazard Assessment Report (HHAR), Human Factors Engineering Analysis (HFEA) and technical test and evaluation reports.

Page 5. Change to read:
b.(5) ... for review and coordination. Safety performance requirements must be incorporated into critical issues and criteria. Issues...

AR 71-9

2-14 CG, TRADOC

Page 6. Change to read:
f. Ensure that the MANPRINT considerations are included in requirements documents; include safety performance requirements based on technical lessons learned from predecessor systems.

AR 385-16

5. Policy

Page 3. Add:
f. Such information will be consolidated in applicable safety handbooks and standards as safety performance requirements and design guidance.

Page 3. Change to read:
k. Applicable training in system safety engineering and mangement will be conducted for all acquisition personnel having a system safety role.

6a. DCSPER

Page 3. Add:
(5) Ensure integrated system safety and human factors engineering review of proposed control measures for severe (catastrophic and critical) hazards that depend on human performance.

6b. Cdr, USASC

Page 3. Add:
(x) Establish and maintain a consolidated Department of the Army (DA) database of safety messages that is accessible to users and supporting safety offices.

h.(3) PMs (Was Materiel Development Commanders)

Page 5. Change to read:
(a) Develop an Army System Safety Management Plan (SSMP), with resource requirements based on the projected life-cycle loss potential of the system. Conduct a tailored system safety program for all developed systems. A System Safety Program Plan (SSPP) is required from contractors or in-house developers for all systems. Ensure...

Page 5. Add:
(g) Develop and maintain safety engineering design guides and standards to ensure that safety and health lessons learned based on past successes and failures are available for design of future systems.

Page 5. Change to read:
(i) ...reduce the risk to acceptable levels. Provide a closed loop system for hazard closeout. Provide the documentation...

DA Pam 385-16

1-8 Hazard severity and probability
Table 1-2 Hazard probability definitions

Page 4. For each level add:

(A) Hazard Probability*	P > 10-2
(B) Hazard Probability*	10-2 > P > 10-3
(C) Hazard Probability*	10-3 > P > 10-4
(D) Hazard Probability*	10-4 > P > 10-6
(E) Hazard Probability*	P < 10-6

* In 1000 hours or 10,000 miles of operation, or 1000 items expended for single-use items or other defined measures of exposure.

Page 4. Add:
1-8d. Care must be taken not to overestimate human reliability. Human factors engineering support should be obtained to estimate human error rates for proposed user-dependent control measures for severe (catastrophic and critical) hazards. Exposure must be considered in addition to hazard probability when evaluating the adequacy of user-dependent control measures.

1-10. Risk Management

Page 4. Change to read:
c. ... order of effectiveness at reducing risk. As a design goal, administrative control measures should be considered only where engineering control measures are not technically feasible or cost effective. Designing for minimum risk...

3-4. System safety management plan

Page 8. Add:
a. (7) Establish the scope and resource requirements of government and contractor system safety programs, based on projected life cycle system loss potential, necessary to adequately minimize mishap potential in the fielded system.

4-1 General

Page 10. Change to read:
b. ... The major efforts of safety testing should be evaluating the adequacy of hazard control measures for identified hazards and identifying and evaluating previously unknown hazards. The hazard tracking system supports testing and is supported by testing. (See Chap. 1, Sec II.)...

4-3 Pretest

Page 10. Change to read:
a. ...included in all reports. The adequacy of hazard control measures for all identified severe (catastrophic and critical) hazards must be verified during testing. The adequacy of user-dependent control measures should be jointly evaluated by system safety, human factors engineers and health hazards specialists. The independent evaluator...

AR 385-40

1-4 b. Commander USASC will

Page 3. Add:
(6) Provide system mishap data to combat and materiel developers and associated contractors.

AR 602-1

1-9 Objectives

Page 1-4. Change to read:
h. In coordination with system safety, provide task analyses and error rate predictions to support determination of whether user-dependent hazard control measures are effective and within human performance limitations.

2-1 General

Page 2-1. Change to read:
f. Identified system hazards, risk assessments, and hazard control measures.

AR 602-2

1-5 The MANPRINT Program

Page 3. Add:
c. (5) ... training, system safety, and health hazard information to support development of technical and management lessons learned; to develop or improve standards, design guides and handbooks.

2-3 SARDA/AAE

Page 4. Add:
g. Ensure that safety and health risk management decisions are made at a level of management commensurate with the level of risk.

2-8 CG, TRADOC

Page 5. Change to read:
e. ... (including safety performance requirements to minimize user-dependent hazard control measures and minimum standards of soldier performance...).

2-9 CG, AMC

Page 6. Add:
k. Testing should verify the resolution of all severe (catastrophic or critical) hazards, including user-dependent control measures.

3-4 MANPRINT in the concept exploration phase

Page 7. Change to read:
d. "...no more training than planned. Control measures for severe hazards (catastrophic or critical) that rely on human performance must be analyzed to ensure that engineering control measures are not technically or financially feasible and that user-dependent control measures are effective and within reasonable human performance capabilities. Where the conceptual system..."

AR 700-142

2-2 Deputy Chief of Staff for Operations and Plans

Page 3. Add:
i. ...and report system performance problems to ASA(RDA). Report system hazards to ASA(RDA) and the Director of Army Safety (DASAF).

2-8 Materiel Developer Commanders

Page 4. Add:
For all post-fielding system evaluations, ensure participation by qualified system safety engineers, and provide observed or user reported system hazards information to the managing authority and the Director of Army Safety (DASAF).

3-2 Objectives

Page 5. Add:
f. Ensure that all identified hazards have been eliminated or controlled with control measures evaluated and residual risks accepted and documented.

3-7 Materiel release prerequisites

Page 6. Change to read:
(3) An approved safety assessment that confirms that all significant hazards have been resolved or risks formally accepted in accordance with 385-16.

AMC/TRADOC PAM 70-2 (Being revised as DA Pam 70-2)

O&O Plan Format

Page 3.12 Add:
5. Provide sufficient detail to ensure that readers understand how the system will be used in the operational environment.

ROC/JSOR Format

Page 4.12 Change to read:
8.e. System Safety. Address safety performance requirements necessary to avoid hazards associated with predecessor systems. Identify tactical and operational

requirements that may impact the safety of the system. List applicable Army, national and host nation safety and health requirements that should be considered in the design.

ROC/JSOR Checklist

Page 4.20 Change to read:
8.e. System Safety.

(1) Are operational or tactical requirements that might increase the probability or severity of mishaps identified?

(2) Are applicable safety design requirements (Army, national or host nation) identified?

(3) Have system safety performance requirements been reviewed by command safety offices of receiving MACOMs?

AS Format

Page 7.12 Change to read:
10. HFE, Safety and Health. Discuss HFE, system safety and health hazard data and design lessons learned throughout the life cyle of predecessor systems or associated with new technologies and materials which may be used in the system design. Summarize risk management plans to ensure that HFE, system safety and health hazard assessment and control are considered throughout the design process. Plans should ensure that control measures for all severe hazards (Hazards with critical or catastrophic severity levels when risk is assessed in accordance with AR 385-16) are verified during testing and that risk management decisions are made at a management level commensurate with the risk and documented. Add the SSMP as an annex to the acquisition strategy. What are the...

Content of AP

Page 8.12 Change to read:
Safety Consideration: Describe in the System Safety Management Plan the scope and resource requirements of government and contractor system safety programs, based on projected life-cycle system loss potential, necessary to adequately minimize mishap potential in the fielded system. This feeder document to the Acquisition Plan should describe the responsibilities and policies of the system safety working group. Discuss the ....

Definitions - Program Documents

Page 9.12 Change to read:
13. System Safety Program Plan (SSPP). The SSPP is a contractor plan that provides uniform requirements...

Page 9.12 Add:
System Safety Management Plan (SSMP). (Use definition from AR385-16.)

Appendix B

Additional Research Suggested by this Study

Appendix B

Additional Research Suggested by this Study

This appendix includes additional research areas identified during the conduct of the system safety management lessons learned study. These research areas address specific issues that were not within the scope of this study.

1. Develop a guide explaining contractual incentive programs for system safety.

2. Provide a standardized methodology for predicting risk probabilities associated with human performance where hazard control depends on administrative control measures.

3. Develop a safety performance specification to minimize potential rollover hazards for military vehicles.

4. Investigate the severity of injuries from mishaps involving troop transport with side facing seats or benches compared to forward facing seats both with and without passenger restraints.

5. Evaluate the degree to which perceived risk affects system acquisition decisions for various types of systems and the impact it has in terms of human and materiel losses. Also evaluate the degree to which research on risk acceptability can be applied to an understanding of risk acceptance by the Army decision maker and the user. Examine differences in risk acceptance levels for engineering vs. administrative control measures on hazards with equal severities. Consider the impact of user risk acceptance levels on mission performance.

6. Using historical information, determine whether perceived risk models could be predictive of potential conflicts between the Army acquisition managers and users, congress or the public regarding acceptability of risks, e.g., swimming of BFVs, agent orange, etc.

7. Develop a system life cycle loss assessment methodology to be used on existing systems to predict loss rates on future systems in order to provide a basis for determining the optimum levels of system safety resources during the acquisition process. This would include direct losses such as injury costs and system damage resulting from mishaps, as well as indirect losses including retrofit costs, and mission or programmatic impacts.

8. Develop efficient, objective measures of system safety performance that could be used as incentives for motivating system safety excellence.

9. Develop system safety design software that could operate in the background of existing computer aided design (CAD) programs to provide designers with relevant safety design lessons learned by subsystem. The software would provide a shell that could be used by the Army and contractors to organize such lessons learned for each commodity area. In use, this software would provide system designers with current system safety design guidance associated with a given commodity.

10. Develop an expert system for Army mishap investigation that could be used to ensure thorough, systematic investigation by unit safety officers or field safety offices. Such a tool would help the investigator to seek the types of information that a group of expert investigators would seek. It would quickly narrow the scope of the investigation and provide greater detail regarding such areas as human performance and material failure. It would focus the investigation and produce the final report for the investigator.

11. Using specific new acquisition programs, evaluate the degree to which the MANPRINT program has, in practice, resolved the systemic causes of mishaps identified in the System Safety Management Lessons Learned study.

PNL-6890
UC-706

DISTRIBUTION

No. of Copies

OFFSITE

G. Gamache (CSSC-RR) (3)
U.S. Army Safety Center
Ft. Rucker, AL 36362-5363

B. Adams (CSSC-SE) (17)
U.S. Army Safety Center
Ft. Rucker, AL 36362-5363

T. Krenelka (2)
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

2 DOE/Office of Scientific and Technical Information

No. of Copies

ONSITE

DOE Richland Operations Office

D. L. Sours

18 Pacific Northwest Laboratory

D. J. Coomes
M. S. Harris
J. C. Lavender
P. J. Pelto
J. A. Piatt (5)
D. A. Seaver
Publishing Coordination (1)
Technical Report Files (5)